应用数学丛书　编码理论

肖国镇　卿斯汉

目　录

第一章 引 论

§1.1 历史的与现实的背景

编码理论导源于现代通信技术与电子计算机技术中差错控制研究的实际需要。美国数学家仙农（C.E.Shannon）在1948年发表的著名论文“通信的数学理论”，开创了一门在现代科学技术中具有重大意义的崭新的学科，即信息论。编码理论是信息论的一个专门分支。

汉明（R.W.Hamming）在1950年发表的论文“检错码与纠错码”是开拓编码理论研究的第一篇论文。这篇论文主要考虑在大型计算机中如何纠正所出现的单个错误。从这种能够纠正单个错误的汉明码过渡到能够纠正多个错误的所谓BCH码，整整经历了10年的时间。因此，可以说60年代是代数编码理论发展的鼎盛时期。70年代出现了高帕码（Goppa *Codes*），从而又把编码理论推向了一个新的高峰。到了80年代，茨伐斯曼（Tsfasman）等人运用代数几何的方法推广了高帕码的思想，指出存在$GF(q)$（$q=p^r$）上的一列码，它超过所谓基尔伯特-瓦尔沙莫夫限（Gilbert-Varshamov *bound*）。这一令人吃惊的结果给编码理论的进一步发展带来了新的希望。除此之外，基于组合理论及有限几何所建立的各种码类，以及在工程技术中具有重大实用价值的卷积码类的研究都大大地丰富了编码理论的研究。

如所周知，一个通信系统可以概括为图1-1所示的模型。来自信源的消息经过信源编码器被变换成能够表达这些消息的符号（为了提高有效性，在对消息进行编码时应当尽量减少多余度）。再经过信道编码器对信源编码器的输出符号进行变换，使变换后的符号具有抗击信道中噪声干扰的能力。最后，经过调制器将信

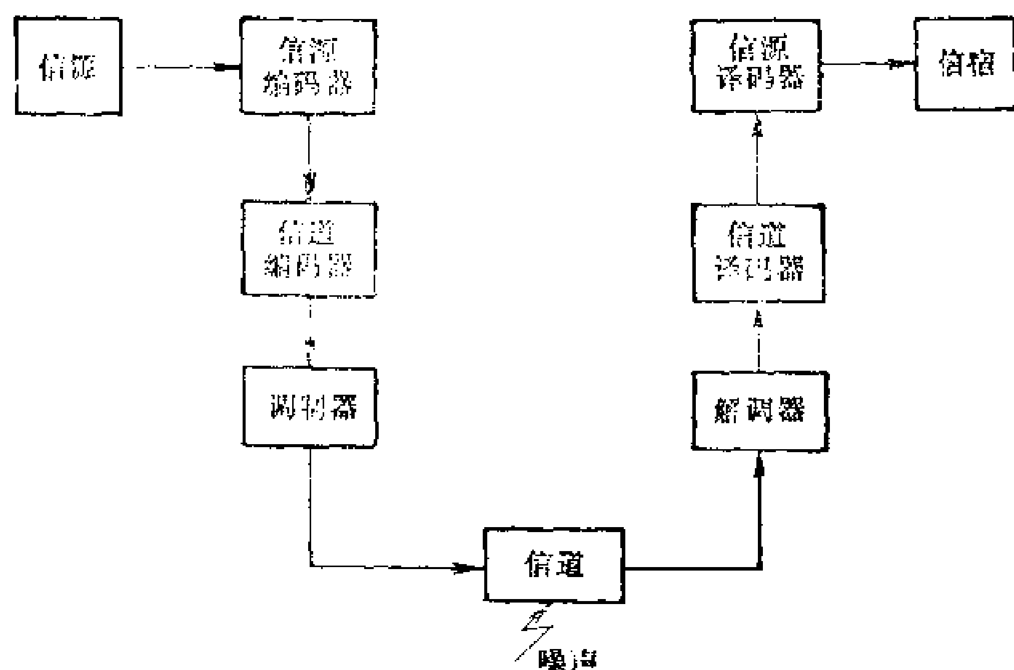

图 1-1

道编码器的输出调制成在带宽、功率及波段等适合于信道传输要求的信号。在收端，经过解调器、信道译码器及信源译码器来恢复发端所发送的消息。本书所要涉及的是信道编码理论，或者说是纠错编码理论。这一理论主要研究具有抗干扰能力的码类的构造及相应的编码及译码方法。

为了说明编码理论在当代空间技术中的应用，最好是看一看美国国家航空和航天管理局（NASA)所发射的探测外行星的"旅行者1号"及"旅行者2号"飞船在1979年及1986年发回地球的彩色照片。在这里即采用了编码技术把许多格点的光暗程度以二元数字传送回地球，经过解调、信道译码及信源译码还原后，便可看到有关木星及天王星的清晰的彩色图象。

从以上的简短回顾，我们可以看出编码理论是当代高科技与基础理论和谐统一、相互促进的一个典范。

§1.2 编码理论的基本思想与仙农信道编码定理

大家知道，在数字电路中，总假定来自信源的信息是二进制数字序列，即 0 — 1 序列。对于这种二进制序列中的符号 0 与 1 可定义加法与乘法如下：

$$\left.\begin{array}{l} 0\oplus 0=0,\ 0\oplus 1=1,\ 1\oplus 0=1,\ 1\oplus 1=0 \\ 0\cdot 0=0,\ 0\cdot 1=0,\ 1\cdot 0=0,\ 1\cdot 1=1 \end{array}\right\} \qquad (1\text{-}1)$$

如此定义的加法与乘法通常称为**模 2 加法与模 2 乘法**，其相应的逆运算——减法和除法，可定义如下：

$$\left.\begin{array}{l} 0\ominus 0=0,\ 1\ominus 1=0,\ 1\ominus 0=1,\ 0\ominus 1=1 \\ \dfrac{0}{1}=0, \qquad \dfrac{1}{1}=1 \end{array}\right\} \qquad (1\text{-}2)$$

由式（1-2）可知，$-1=1$。因此，在模 2 算术中，加法与减法是一样的。并且，平常算术中的运算规律，诸如结合律，交换律及分配律等，在这里依然有效。

两个符号 0，1 所构成的集合，如果与它所定义的算术运算式（1-1）与式（1-2）联系起来，便称为**二元域（或二进制域）**，记为 $GF(2)$。

对于来自信源的信息序列（即二进制数字序列），首先将其分成消息组，每个消息组由 k 位接续的信息数字组成，从而总共有 2^k 种不同的消息。其次，编码器按照一定的规则把每个消息变换成较长的 n 位（$n>k$）二进制数字组，称其为**码字**。由这 2^k 个消息所获得的 2^k 个码字的全体，便称为**码组长为 n，信息位为 k 的分组码**。每个消息所增加的 $n-k$ 个数字称为**多余数字**，它们不含有任何新的消息，其作用仅在于使码字在有干扰的信道中传输时能够修正传输中产生的错误。称比值

$$R=\frac{k}{n}$$

为该分组码的**信息率**。或者，更为一般地，假定有 s 个不同的消息，每个消息由 k 位二进数字组成，将每个消息增加 $n-k$ 个多余

数字，从而得到含 s 个码字的分组码 C。称比值

$$R=\frac{\log_2|C|}{n}$$

为该分组码 C 的**信息率**，其中 $|C|$ 代表该分组码中码字的总数，即为 s。当 $s=2^k$ 时，便有 $R=k/n$。

为什么将消息数字适当增加些多余数字，就会提高消息在传输过程中的抗干扰能力呢？这是常识范围内所能想像到的。比如你见到一个英语字母组合 *Infomation*，马上会想到它是英语单词 *Information* 之误。但是，如果你见到 *tall* 这个字母组合，便无法猜出它是 *tall* 之误，还是 *tell* 或 *till* 之误。道理很简单，长的字即使其中有一两个字母错了，它还是像原来那个字多于像其它的字。短的字母则不然，印错的字可能与许多另外的字都相象。因此，编码的基本思想就是将原来要传送的消息数字适当加长，以便使所有传送的消息在传输过程中所产生的错误容易辨认及纠正。

把消息数字适当加长使其变换为码字的过程，称为**编码**。把接收的数字组按照一定的准则恢复成码字的过程，称为**译码**。

一个合理的译码准则是所谓**极大后验概率译码准则**。当接收端收到长为 n 的数字组 $\mathbf{r}$（称为接收字）时，对于所有可能的码字 $\mathbf{c}_i$，计算全部条件概率 $p(\mathbf{c}_i|\mathbf{r})$，$i=1,2,\cdots,s$，若某一码字 $\mathbf{c}_i$ 使 $p(\mathbf{c}_i|\mathbf{r})$ 最大，便把 $\mathbf{r}$ 译作 $\mathbf{c}_i$。这就是所谓最大后验概率译码准则。但条件概率 $p(\mathbf{c}_i|\mathbf{r})$ 实际上不易计算。为此，依概率计算法则可将 $p(\mathbf{c}_i|\mathbf{r})$ 写成

$$p(\mathbf{c}_i|\mathbf{r})=\frac{p(\mathbf{c}_i)\,p(\mathbf{r}|\mathbf{c}_i)}{p(\mathbf{r})}$$

如果进一步假设全部码字在信道上传送是等概率的：

$$p(\mathbf{c}_i)=\frac{1}{s},\quad i=1,2,\cdots,s$$

便有

$$p(\mathbf{c}_i|\mathbf{r})=\frac{p(\mathbf{r}|\mathbf{c}_i)}{s\,p(\mathbf{r})}$$

由此可见，当且仅当 $p(\mathbf{r}|\mathbf{c}_i)$ 最大时，$p(\mathbf{c}_i|\mathbf{r})$ 为最大。按

$p(\mathbf{r}|\mathbf{c}_i)$最大的译码方案称为**极大似然译码准则**。从信息论的观点看，当一个信道给定时，意味着转移概率$p(\mathbf{r}|\mathbf{c}_i)$是完全确定的。不过，按极大似然译码准则进行译码，这种算法的复杂度仍然很大。有人估计，对于$n=10$，$R=1/2$的二进制码，按极大似然译码准则的计算量竟达至10^{15}次之多！

为进一步简化计算，考虑图 1-2 所示的二元对称信道。在这种信道中，发 0 收 0 或发 1 收 1（传输正确）的概率均为 q，而发 0 收 1 或发 1 收 0（传输错误）的概率均为$p=1-q$，并且假设$p<\frac{1}{2}$。这种信道的转移概率矩阵是

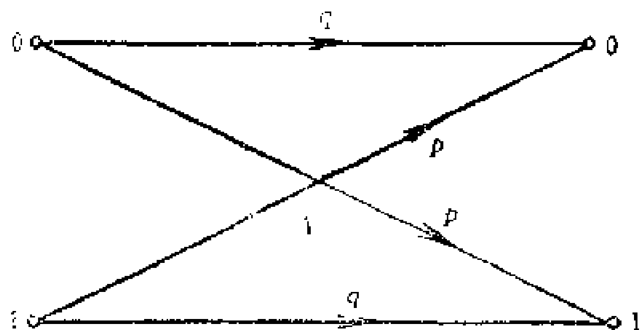

图 1-2

$$T=\begin{bmatrix} p(0|0) & p(1|0) \\ p(0|1) & p(1|1) \end{bmatrix}=\begin{bmatrix} q & p \\ p & q \end{bmatrix}$$

称这种信道为**二元对称信道**。进一步还假定：在传输中每个符号传输正确与否与别的符号传输正确与否是两个独立的事件。

让我们再回到转移概率$p(\mathbf{r}|\mathbf{c}_i)$的计算上来。设$d_i$代表$\mathbf{r}$与$\mathbf{c}_i$对应位分量不相同的数目，称之为$\mathbf{r}$与$\mathbf{c}_i$之间的**汉明距离**。例如$\mathbf{r}=(01001)$与$\mathbf{c}_i=(10111)$之间的汉明距离为 4 。于是，在上述假定下便有

$$p(\mathbf{r}|\mathbf{c}_i)=p^{d_i}q^{n-d_i}$$

根据微积分中极值理论不难看出，当且仅当d_i最小时，$p(\mathbf{r}|\mathbf{c}_i)$最大。由此，我们又得出一个译码方案：收到$\mathbf{r}$后，在全部码字$\mathbf{c}_i$（$i=1, 2, \cdots, s$）中寻找与$\mathbf{r}$的汉明距离最近的$\mathbf{c}_i$判决为原来发送的码字（这就是我们前面提到过的印错的字更像谁的问题）。称这种译码方案为**最小距离译码准则**。

总之，在二元对称信道相应的假定下，极大后验概率译码准

则、极大似然译码准则与最小距离译码准则是一回事情。

紧接着的一个问题便是按照一定的译码方案来计算错误译码概率的问题。一个合理的译码方案均应是使错误译码概率为最小的方案。

在二元对称信道中，长为 n 的码字在传输中全然无误的概率应当是 q^n。如果给定的码能纠正至多 1 个错误，这种模式共有 $\binom{n}{1}=n$ 种，每一种产生的概率均为 pq^{n-1}。因而对于那种能纠正至多 1 个错误的信道及相应的码，接收端正确译码的概率应当是 q^n+npq^{n-1}。一般，对于那种能纠正至多 t 个错误的码，接收端正确译码的概率应当是

$$p_c=\sum_{i=0}^{t}\binom{n}{i}p^iq^{n-i}$$

而错误译码的概率应当是

$$p_e=1-p_c=\sum_{i=t+1}^{n}\binom{n}{i}p^iq^{n-i} \tag{1-3}$$

这一错误译码概率简称为**误码率**。

例如，考虑所谓**重复码**，把待发送的信息数字 0 与 1 分别重复$2N+1$次：

$$0\mapsto\underbrace{0\ 0\cdots0}_{2N+1};\quad 1\mapsto\underbrace{1\ 1\cdots1}_{2N+1}$$

译码按照所谓**大数逻辑准则**，即当接收到 $r=a_0a_1\cdots a_{2N}$ 时，若其中 1 的个数多于N个，则将r译作 $11\cdots1$，否则便将r 译作 $00\cdots0$。这种译码方案显然是最小距离译码方案。按这种方案错误译码的概率应当是（注意 $p<1/2$）

$$p_e(N)=\sum_{k=0}^{N}\binom{2N+1}{k}q^kp^{2N+1-k}\leqslant(pq)^N\sum_{k=0}^{N}\binom{2N+1}{k}$$
$$=(pq)^N2^{2N}=(4pq)^N$$

注意当 $p=1/2$ 时，$4pq=4p(1-p)$ 取得最大值1，故当

$p < \frac{1}{2}$ 时，$4pq < 1$。因而当 $N \to \infty$ 时，$p_e(N) \to 0$。这表明，只要增大信息的重复次数便可使误码率变得任意小。但是，这样做便使该码的信息率 $R = 1/(2N+1)$ 变得任意小，在实践上是很不经济的。

令人振奋的是仙农在 40 年代末确立了下述的深刻定理。

仙农信道编码定理 每一个信道都有一个确定的信道容量 C（它标志该信道最大传输信息的能力。例如对于二元对称信道，$C = 1 + p\log_2 p + q\log_2 q$）。对于任意的 $\varepsilon > 0$ 及给定的 R，$0 < R < C$，必存在一个分组长度 n 足够大而信息率为 R 的码，当采用最大似然译码准则时可使错误译码概率 $p_e < \varepsilon$。

这一定理的证明，读者可在信息论的专著中找到。为了说明这一定理的结果是可信的，我们举一个例子说明在信息率 R 不变的情况下，可以通过增大码长 n 使误码率降低。假定 $R = 1/2$，$p = 0.01$，$q = 0.99$，考虑重复码：$0 \mapsto 00$；$1 \mapsto 11$。按照大数逻辑译码准则，当且仅当所收到的 $r = a_0a_1$ 中两位均无错时，才能正确译码。因而正确译码的概率 $p_c = q^2 = 0.9801$，错误译码的概率 $p_e = 1 - p_c = 0.0199$。假定我们等到传 2 个信息元之后才一并传 4 个元（后面 2 个是多余码元）。按下述规则编码：

$$00 \longmapsto 0000,$$
$$01 \longmapsto 0111,$$
$$10 \longmapsto 1001,$$
$$11 \longmapsto 1110。$$

亦即假定码字 $c = a_0a_1a_2a_3$ 之后两位多余码元按下述规则添加：

$$a_2 = a_1 \qquad (1\text{-}4)$$
$$a_3 = a_0 + a_1$$

由此不难看出，如果采用译码算法：当式(1-4)成立时，认为收到的 $r = a_0a_1a_2a_3$ 无错；当式(1-4)不成立时，认为 a_3 无错而 a_0，a_1，a_2 中有一位错，则这种码可纠正前 3 位中不多于 1 个的错误。事实上，如果式(1-4)中 $a_2 \neq a_1$，$a_3 = a_0 + a_1$，则可断定 a_2 有错。同理，当 $a_2 = a_1$ 而 $a_3 \neq a_0 + a_1$ 时，a_0 有错。最后，当

$a_2 \neq a_1$，$a_3 \neq a_0 + a_1$ 时，a_1 有错。这种码的信息率 R 仍为 $1/2$，但它的正确译码概率却为 $p_c = q^4 + 3q^3p = 0.9897$，从而错误译码概率 $p_e = 1 - p_c = 0.0103$，比以前明显地减少了。这正是仙农信道编码定理的重大价值所在。

由于这一定理的证明是非构造性，并告诉我们如何去寻找这种性能良好的码，因而几十年来在信息传输技术实际需要的推动下，使编码理论的发展获得了经久不衰的生命力。

§1.3　码的纠错能力与检错能力

在编码理论中的一个最重要的概念是所谓汉明距离的概念。假设 $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)$ 与 $\boldsymbol{y} = (y_1, y_2, \cdots y_n)$ 是分量取在 $GF(2)$ 上的两个 n 维向量，有时也把这种 n 维向量称为 n 重，或者称为 n 维空间中的点。

定义1.3.1　设 $\boldsymbol{x}$ 与 $\boldsymbol{y}$ 是分量取在 $GF(2)$ 上的两个 n 重，称 $\boldsymbol{x}$ 与 $\boldsymbol{y}$ 中对应分量不相同的数目为 $\boldsymbol{x}$ 与 $\boldsymbol{y}$ 之间的汉明距离，记为 $d_H(\boldsymbol{x}, \boldsymbol{y})$ 或 $d(\boldsymbol{x}, \boldsymbol{y})$。

例如，$d((1011), (0101)) = 3$

不难看出：

$$d(\boldsymbol{x}, \boldsymbol{y}) = |\{ i \mid 1 \leqslant i \leqslant n, \ x_i \neq y_i \}|$$

此处 $|\{\cdot\}|$ 代表集合 $\{\cdot\}$ 中元素的数目。

定理1.3.1　$GF(2)$ 上的 n 重之间的汉明距离服从距离公理

(1)　$d(\boldsymbol{x}, \boldsymbol{y}) \geqslant 0$；$d(\boldsymbol{x}, \boldsymbol{y}) = 0$ 当且仅当 $\boldsymbol{x} = \boldsymbol{y}$

(2)　$d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$

(3)　$d(\boldsymbol{x}, \boldsymbol{z}) \leqslant d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z})$

证明　性质(1)、(2)十分明显，只需证(3)。对于 $GF(2)$ 上的任意两个 n 重 $\boldsymbol{x}$ 与 $\boldsymbol{y}$，不难看出

$$d(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} (x_i \oplus y_i)$$

此处Σ是按普通实数相加。并且显然有

$$x_i \oplus y_i \leqslant x_i + y_i$$

于是

$$d(\boldsymbol{x}, \boldsymbol{z}) = \sum_{i=1}^{n} (x_i \oplus z_i) = \sum_{i=1}^{n} [(x_i \oplus y_i) \oplus (y_i \oplus z_i)]$$

$$\leqslant \sum_{i=1}^{n} [(x_i \oplus y_i) + (y_i \oplus z_i)]$$

$$= \sum_{i=1}^{n} (x_i \oplus y_i) + \sum_{i=1}^{n} (y_i \oplus z_i)$$

$$= d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z})$$

（证毕）

因此，在 $GF(2)$ 上的一些 n 重的集合上定义了汉明距离后，便使这种集合构成距离空间。

汉明距离的概念与码的纠错能力与检错能力密切相关。

定义1.3.2 如果分组码 C 能够纠正所有不超过 t 个独立的随机错误，但不能纠正所有多于 t 个独立的随机错误，则称该分组码 C 的纠错能力为 t。

如果一个分组码 C 只含一个 n 重，即 $|C|=1$，则称此分组码是平凡的。今后我们所讨论的分组码均假定是非平凡的。

定义1.3.3 一个分组码 C 的最小汉明距离是指

$$d(C) \triangleq \min_{\substack{\boldsymbol{x},\boldsymbol{y}\in C \\ \boldsymbol{x}\neq \boldsymbol{y}}} d(\boldsymbol{x}, \boldsymbol{y})$$

下面的定理给出判定分组码纠错能力的重要标志。

定理1.3.2 分组码 C 的纠错能力为 t 的充分必要条件是

$$2t+1 \leqslant d(C) \leqslant 2t+2 \tag{1-5}$$

证明 假定式（1-5）成立。设 $\boldsymbol{v}$ 为发送码字，$\boldsymbol{r}$ 为接收的 n 重，且 $d(\boldsymbol{v}, \boldsymbol{r}) \leqslant t$。若 $\boldsymbol{v}'$ 为任意码字，$\boldsymbol{v} \neq \boldsymbol{v}'$，则由定理1.3.1之（3），有

$$d(\boldsymbol{v}, \boldsymbol{r}) + d(\boldsymbol{r}, \boldsymbol{v}') \geqslant d(\boldsymbol{v}, \boldsymbol{v}') \geqslant 2t+1$$

因此

$$d(v', r) \geqslant (2t+1) - d(v, r) \geqslant 2t + 1 - t > t \geqslant d(v, r)$$

这表明码 C 能纠正所有不超过 t 个独立的随机错误。图 1-3(a) 是这一事实的几何说明。

其次，证明码 C 不能纠正所有多于 t 个独立的随机错误。由假设，$d(C) \leqslant 2t+2$。当 $d(C) < 2t+2$ 时，由式(1-5)有 $d(C) = 2t+1$。于是存在码字 v，v'，$v \neq v'$，使 $d(C) = d(v, v') = 2t+1$。不妨设 v 与 v' 中 $d(C)$ 个对应不相同的分量如下：

$v_{i_1} \neq v'_{i_1}$，$v_{i_2} \neq v'_{i_2}$，$\cdots$，$v_{i_l} \neq v'_{i_l}$，$l = d(C)$。现在作一个 n 重 $r = (r_1, r_2, \cdots, r_n)$，它是由 v' 按下述方式改变 t 个分量得来：

$$r_{i_1} = v_{i_1}, \quad r_{i_2} = v_{i_2}, \quad \cdots, \quad r_{i_t} = v_{i_t}$$

r 中其余分量保持与 v' 之对应分量相同。于是

$$d(v, r) = d(v, v') - t = t + 1 > t = d(v', r)$$

若以 v 作发送码字，r 为接收的 n 重（造成 $t+1$ 个差错），则 r 不是与 v 更接近，而是与 v' 更接近。(见图 1-3(b))。

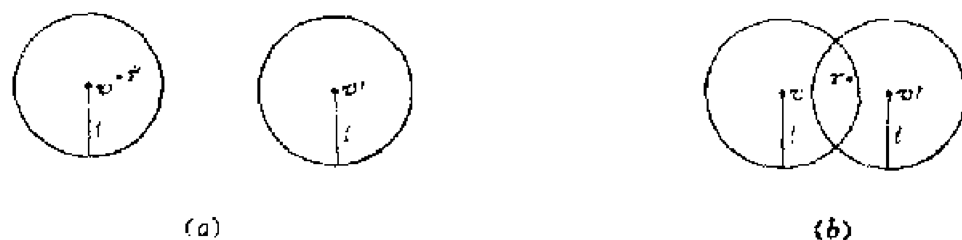

图 1-3

同理，当 $d(C) = 2t+2$ 时，存在码字 v，v' 使 $d(C) = d(v, v') = 2t+2$。改变 v' 中 $t+1$ 个分量得 n 重 r，使

$$d(v, r) = d(v', r) = t + 1$$

于是，当发送 v 而接收到 r 时，r 与 v 及 v' 同样接近，因而无法按最小距离准则译码。

现在证明条件的必要性。假定码C之纠错能力为t。如果式(1-5)不成立，则因$d(C)$为正整数，必有非负整数t'，$t' \neq t$，满足

$$2t'+1 \leqslant d(C) \leqslant 2t'+2$$

由前段充分性的证明，该码的纠错能力为$t' \neq t$。 〈证毕〉

注意，不等式(1-5)表明

$$t \leqslant \frac{d(C)-1}{2} \leqslant \frac{2t+1}{2} < t+1$$

因此，由定理1.3.2可知，一个分组码C的纠错能力恒为$[(d(C)-1)/2]$。这里符号$[x]$代表实数x的整数部分，即不超过x的最大整数。例如，$[1.5]=1$，$[-1.2]=-2$等等。

推论1.3.2.1 分组码C的纠错能力至少为t的充分必要条件是

$$d(C) \geqslant 2t+1 \tag{1-6}$$

证明 若式(1-6)成立，则由定理1.3.2的证明可知，码C能纠正所有不超过t个独立的随机错误。反之，若式(1-6)不成立，即$d(C) \leqslant 2t$，则由定理1.3.2的证明，码C不能纠正所有t个独立的随机错误。 〈证毕〉

从几何观点看，当且仅当以分组码C中的每一码点为中心，以t为半径所作的球

$$S_t(v)=\{r \mid d(v, r) \leqslant t\}$$

彼此分离，即满足

$$\bigcap_{v \in C} S_t(v)=\varnothing$$

时，该码能纠正所有不多于t个独立的随机错误(见图1-3(a))。

在本节的最后，我们讨论分组码的检错能力。

定义1.3.4 如果分组码C能够检测出（发现）所有不多于l个独立的随机错误，但不能检测出所有多于l个独立的随机错误，则称该分组码C的检错能力为l。

从几何观点看，当且仅当以分组码C中的每一码点为中心，

以 l 为半径所作的球 $S_l(v)$ 除球心外不含 C 中任何其它码点时，该码能检测出所有不多于 l 个独立的随机错误（见图 1-4）。

定理1.3.3 分组码 C 的检错能力为

$$l=d(C)-1$$

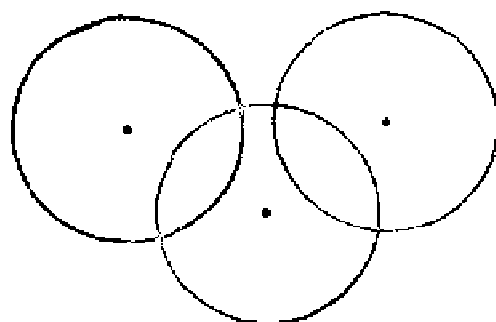

图 1-4

证明 首先证明当错误个数 $\leqslant l$ 时，信道不能把一个码点错传成另一码点。事实上，若 v，v' 为码点，$v\neq v'$，则

$$d(v,\ v')\geqslant d(C)=l+1$$

因此，对于任何接收的 n 重 r，只要 $d(v,\ r)\leqslant l$，必有 $r\neq v'$。因此该分组码能够检测出所有不多于 l 个独立的随机错误。

其次证明译码器不能检测出所有多于 l 个独立的随机错误。事实上，存在码点 v，v'，$v\neq v'$，使 $d(v,v')=d(C)=l+1$。假定 v 为发送码点，v' 为接收的 n 重。因 v' 亦为码点，故译码器判定未发生错误，从而这种错误无法检测出来。 〈证毕〉

例1.3.1 考虑 § 1.2 中的重复码 C

$$0\longmapsto\underbrace{0\ 0\cdots0}_{2N+1};\quad 1\longmapsto\underbrace{1\ 1\cdots1}_{2N+1}$$

显然 $d(C)=2N+1$。因此该码的纠错能力为 $[(d(C)-1)/2]=N$。这是我们已经知道的事实。另外，该码的检错能力为 $d(C)-1=2N$。

例1.3.2 考虑分组码

$$C=\{(0000),\ (0111),\ (1001),\ (1110)\}$$

显然 $d(C)=2$。该码的纠错能力为 0 。事实上，正如在 § 1.2 中所看到的，这种码只能纠正前 3 位的单个错误而不能纠正第 4 位的单个错误。该码的检错能力为 1 。

从上面的讨论我们看到，要增大码的纠错能力，必须构造那种分组码 C，使 $d(C)$ 尽可能地大。同时，为使码的信息率 R 尽可能地大，还需要求 $n\approx k$（n 为码长，k 为信息位）。这就是

编码理论的中心课题之一。

在码的最小汉明距离一定的条件下，同时想使码的纠错能力及检错能力都尽量大，这是对立的统一。一般，为使一个分组码 C 能够纠正所有不多于 t 个独立的随机错误同时又能另外检测出所有大于 t 且不超过 l 个独立的随机错误（$l>t$），可设计码 C 的最小汉明距离为

$$d(C)=t+l+1$$

由此不难看出，该码的纠错能力

$$\left[\frac{d(C)-1}{2}\right]=\left[\frac{t+l}{2}\right]\geqslant t$$

检错能力为 $t+l$。

从几何观点看，相当于对码 C 的每一个码点 v 分别作以 v 为中心，半径为 t 及 $t+l$ 的两个码球 $S_t(v)$ 及 $S_{t+l}(v)$，使得在 t 的范围内所有码球彼此分离：

$$\bigcap_{v\in C} S_t(v)=\varnothing$$

而在 $t+l$ 范围内每一个码球 $S_{t+l}(v)$ 除中心外不含另外的码点。于是，当且仅当上述情况下，该码对于 t 范围内的错误可以纠正，而在 $t+1$ 到 $t+l$ 范围内的错误可检测出（见图 1-5）。

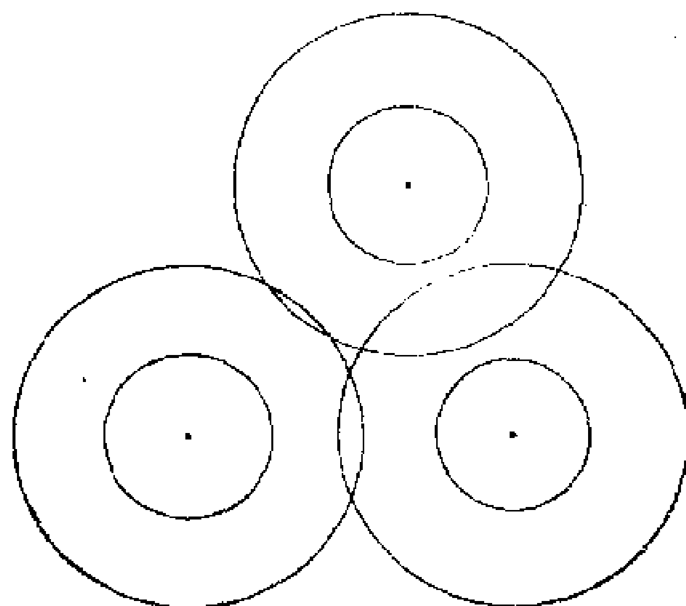

图 1-5

§1.4 q元信道的编码问题

前几节所讨论的问题均假定来自信源的信息用2元符号0，1编制成信息序列。代替由0，1构成的二元域，我们可以考虑信源的信息由q个元素a_0，a_1，…，a_{q-1}所构成的q元域。这种域记为$GF(q)$，它的代数理论以后详细讨论。对于q元域的情形，我们仍然可以建立相应的编码与译码的概念。例如，我们可以建立q元对称信道的概念，这种信道的转移概率矩阵是

$$T=\begin{bmatrix} p(a_0|a_0) & p(a_1|a_0)\cdots p(a_{q-1}|a_0) \\ p(a_0|a_1) & p(a_1|a_1)\cdots p(a_{q-1}|a_1) \\ \vdots & \vdots \quad \cdots \quad \vdots \\ p(a_0|a_{q-1}) & p(a_1|a_{q-1})\cdots p(a_{q-1}|a_{q-1}) \end{bmatrix}$$

$$=\begin{bmatrix} 1-p & p/(q-1) \cdots p/(q-1) \\ p/(q-1) & 1-p \quad \cdots p/(q-1) \\ \vdots & \vdots \quad \cdots \quad \vdots \\ p/(q-1) & p/(q-1)\cdots \quad 1-p \end{bmatrix}$$

亦即对于每一个信息符号a_i，正确传送的概率均为$1-p$（其中$p<1/2$，从而$1-p>1/2$），而错误传送的概率均为$p/(q-1)$。

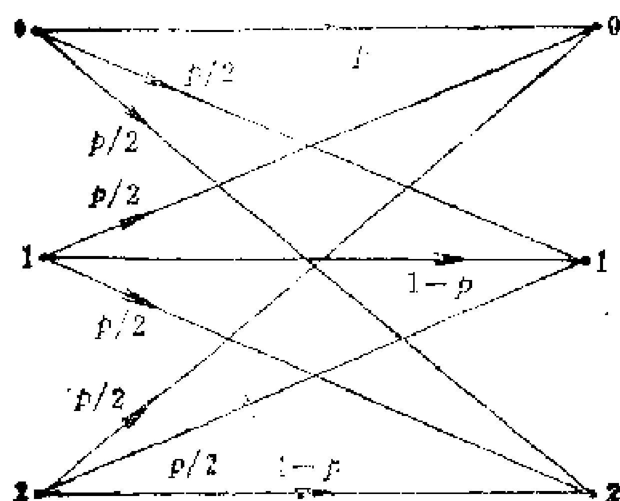

图 1-6

作为例子，考虑由模 3 的剩余类 0，1，2 所构成的 3 元域(其中算术运算规则是 $1+2=0$，$-1=2$，$2+2=1$，$2\cdot 2=1$，等等)。相应的 3 元对称信道如图 1-6 所示。

同样，对于分量取在 q 元域 $GF(q)$ 上的两个 n 重 $\boldsymbol{x}$ 与 $\boldsymbol{y}$，我们仍然可以定义汉明距离

$$d(\boldsymbol{x},\ \boldsymbol{y}) \triangleq |\{i \mid 1 \leqslant i \leqslant n,\ x_i \neq y_i\}|$$

在此，定理 1.3.1 仍然成立。

以此为基础，有关分组码的纠错能力及检错能力的相应结果对于 q 元域 $GF(q)$ 仍然成立。

第二章　从线性空间到线性码

§2.1　线性空间的概念

本书主要论述线性码，从线性空间引入线性码是最为自然的。

众所周知，普通的向量具有两种运算：向量加法，数与向量的乘法。但是，具有这两种运算的系统不只是向量，诸如矩阵、多项式等皆有这两种运算。把这些表面上看来不尽相同的对象的共性抽象出来，对于它们所具有的基本运算规律进行统一的研究，就导致了线性空间的概念。

定义2.1.1　设V是一个集合，假定在V中任意两个元素之间都定义了加法，并且对任意的数与V中的任意元素都定义了乘法[1]。设$\boldsymbol{x}$，$\boldsymbol{y}$，$\boldsymbol{z}\in V$，α，β，γ等表示普通的数。如果这两种运算满足下述条件，则称集合V为一个**线性空间**：

(1) 1°　$\boldsymbol{x}+\boldsymbol{y}=\boldsymbol{y}+\boldsymbol{x}$（交换律）；

2°　$(\boldsymbol{x}+\boldsymbol{y})+\boldsymbol{z}=\boldsymbol{x}+(\boldsymbol{y}+\boldsymbol{z})$（结合律）；

3°　V中存在元素$\boldsymbol{0}$，使得$\boldsymbol{x}+\boldsymbol{0}=\boldsymbol{x}$，对一切$\boldsymbol{x}\in V$。元素$\boldsymbol{0}$称作**零元素**；

4°　对于V中任一元素$\boldsymbol{x}$，存在着用$(-\boldsymbol{x})$表示的一个元素，满足$\boldsymbol{x}+(-\boldsymbol{x})=\boldsymbol{0}$。

(2) 1°　$1\cdot\boldsymbol{x}=\boldsymbol{x}$；

2°　$\alpha(\beta\boldsymbol{x})=(\alpha\beta)\boldsymbol{x}$。

(3) 1°　$(\alpha+\beta)\boldsymbol{x}=\alpha\boldsymbol{x}+\beta\boldsymbol{x}$；

2°　$\alpha(\boldsymbol{x}+\boldsymbol{y})=\alpha\boldsymbol{x}+\alpha\boldsymbol{y}$。

根据这个定义，平面（或空间）上的全体向量显然构成线性

---

[1] 代数中所定义的运算包含着封闭性的要求，即假定V中任意两个元素相加，以及任意数与V中任意元素相乘的结果仍为V中的元素。

空间。从这一直观角度出发，我们常常把线性空间V中的元素称为**向量**，而把V称为**向量空间**。其次，在线性空间的定义中所说的数，根据需要可视为实数、复数或$GF(2)$中的元素。今后，当我们介绍了近世代数中域的概念之后，也可以把这里所说的数视为任意一个域中的元素。

例2.1.1 假设V_n是由取自$GF(2)$的n个元素的序列

$\boldsymbol{x}=(x_1, x_2, \cdots, x_n)$，$x_i\in GF(2)$，$i=1, 2\cdots, n$的全体所构成。$V_n$中二元素$\boldsymbol{x}=(x_1, x_2, \cdots, x_n)$与$\boldsymbol{y}=(y_1, y_2, \cdots, y_n)$之和定义为

$\boldsymbol{x}+\boldsymbol{y}\triangleq(x_1\oplus y_1, x_2\oplus y_2, \cdots, x_n\oplus y_n)$

数$\lambda\in GF(2)$与$\boldsymbol{x}\in V$之积定义为

$$\lambda\boldsymbol{x}\triangleq(\lambda x_1, \lambda x_2, \cdots, \lambda x_n)$$

不难看出，V_n构成一个线性空间。此处，零元素是$\mathbf{0}=(0, 0, \cdots, 0)$。常常称$V_n$为**$n$维向量空间**，这一空间在编码理论中特别重要。

以下称线性空间中所定义的那两种运算，即向量加法和数乘向量，为**线性运算**。

定义2.1.2 设S为线性空间V的一个子集。如果S按照V中所定义的线性运算仍然构成一个线性空间，则称S为线性空间V的**子空间**。

下述定理可以用于判断线性空间的子集是否为子空间。

定理2.1.1 设V是线性空间，S是V的子集，则S是V的子空间当且仅当

（1）若$\boldsymbol{x}, \boldsymbol{y}\in S$，则$\boldsymbol{x}+\boldsymbol{y}\in S$；

（2）若$\boldsymbol{x}\in S$，λ是任意数，则$\lambda\boldsymbol{x}\in S$。

证明 必要性是显然的，因为条件（1），（2）若不成立，则S不是一个线性空间。

现在证明充分性。假定条件（1），（2）成立，我们证明S满足线性空间定义中的（1）～（3）。条件（1）1°，2°及（2），（3）显然满足，因为S的元素也是V的元素。因此，只需验证

条件(1)之3°，4°。设$\boldsymbol{x}\in S$，由本定理的条件（2）知，$0\boldsymbol{x}=\boldsymbol{0}\in S$，$(-1)\boldsymbol{x}=-\boldsymbol{x}\in S$，可见条件(1)的3°，4°确实成立。

〈证毕〉

不难看出，定理中的条件（1）和（2）可以合并为一个条件，即若$\boldsymbol{x}$，$\boldsymbol{y}\in S$，λ_1和λ_2是任意数，则$\lambda_1\boldsymbol{x}+\lambda_2\boldsymbol{y}\in S$。

对于每一个线性空间V，都有两个明显的子空间：一个是仅由V中的零元素所构成的**零子空间**，一个是V本身。我们称它们为**平凡子空间**，而其它的线性子空间叫作**非平凡子空间**。

当线性空间V中所涉及的数取自$GF(2)$时，称V是**$GF(2)$上的线性空间**。此时，定理中的条件（2）退化为$\boldsymbol{0}\in S$。但这个条件可由定理中的条件（1）推出。事实上，任取$\boldsymbol{x}\in S$，则

$\boldsymbol{x}+\boldsymbol{x}=1\cdot\boldsymbol{x}+1\cdot\boldsymbol{x}=(1+1)\boldsymbol{x}=0\cdot\boldsymbol{x}=\boldsymbol{0}\in S$。因此，**$GF(2)$上的线性空间$V$的子集$S$构成子空间当且仅当若$\boldsymbol{x}$，$\boldsymbol{y}\in S$，则$\boldsymbol{x}+\boldsymbol{y}\in S$。**

例2.1.2 考虑$GF(2)$上的4维线性空间V_4，设它的一个子集

$S=\{(0000),(0101),(1010),(1111)\}$

容易验证，S中任意两个向量之和仍在S中。因此，S是V_4的一个子空间。

定义2.1.3 设V是线性空间。对于V中的元素组

$$\boldsymbol{x}_1,\ \boldsymbol{x}_2,\ \cdots,\ \boldsymbol{x}_s,$$

若存在一组不全为零的数$k_i(i=1,2,\cdots,s)$，使

$$k_1\boldsymbol{x}_1+k_2\boldsymbol{x}_2+\cdots+k_s\boldsymbol{x}_s=\boldsymbol{0} \tag{2-1}$$

则称该元素组是**线性相关的**。否则仅当k_1，k_2，…，k_s全为零式(2-1)才成立时，则称该元素组是**线性独立的**，或**线性无关的**。

定义2.1.4 如果在线性空间V中存在n个线性无关的元素，并且在V中没有多于n个元素所构成的线性独立元素组时，则称线性空间V的维数为n，并称V为**n维线性空间**。

如果在线性空间V中可以找到任意多个线性独立的元素，则

称V是**无限维线性空间**，这不属于本书讨论的范围。

定义2.1.5 如果在线性空间V中存在一组线性独立的向量

$$\boldsymbol{e}_1,\ \boldsymbol{e}_2,\ \cdots,\ \boldsymbol{e}_n \tag{2-2}$$

使V中任意向量$\boldsymbol{x}$皆可表示为向量组（2-2）的线性组合

$$\boldsymbol{x}=x_1\boldsymbol{e}_1+x_2\boldsymbol{e}_2+\cdots+x_n\boldsymbol{e}_n \tag{2-3}$$

则称向量组（2-2）为空间V的一个**基底**，并称（2-3）中之x_1，x_2，…，x_n为向量$\boldsymbol{x}$的**坐标**。

为了说明基底向量的个数与空间维数之间的关系，我们给出下面的引理。

引理2.1.1 设$\boldsymbol{e}_1$，$\boldsymbol{e}_2$，…，$\boldsymbol{e}_n$为线性空间V的n个线性独立的向量。如果空间V中s个向量所构成的向量组

$$\boldsymbol{x}_1,\ \boldsymbol{x}_2,\ \cdots,\ \boldsymbol{x}_s,\quad s>n$$

中的每一个向量皆可表为向量$\boldsymbol{e}_1$，$\boldsymbol{e}_2$，…，$\boldsymbol{e}_n$的线性组合，则向量组$\boldsymbol{x}_1$，$\boldsymbol{x}_2$，…，$\boldsymbol{x}_s$线性相关。

证明 由假设

$$\left.\begin{aligned}\boldsymbol{x}_1&=a_{11}\boldsymbol{e}_1+a_{12}\boldsymbol{e}_2+\cdots+a_{1n}\boldsymbol{e}_n\\ \boldsymbol{x}_2&=a_{21}\boldsymbol{e}_1+a_{22}\boldsymbol{e}_2+\cdots+a_{2n}\boldsymbol{e}_n\\ &\cdots\\ \boldsymbol{x}_s&=a_{s1}\boldsymbol{e}_1+a_{s2}\boldsymbol{e}_2+\cdots+a_{sn}\boldsymbol{e}_n\end{aligned}\right\} \tag{2-4}$$

判断是否存在不全为零的数λ_1，λ_2，…，λ_s，使

$$\lambda_1\boldsymbol{x}_1+\lambda_2\boldsymbol{x}_2+\cdots+\lambda_s\boldsymbol{x}_s=\boldsymbol{0}$$

相当于考察下列齐次线性方程组是否有非零解

$$\left.\begin{aligned}a_{11}\lambda_1+a_{21}\lambda_2+\cdots+a_{s1}\lambda_s&=0\\ a_{12}\lambda_1+a_{22}\lambda_2+\cdots+a_{s2}\lambda_s&=0\\ \vdots\qquad\quad \cdots\qquad &\ \vdots\\ a_{1n}\lambda_1+a_{2n}\lambda_2+\cdots+a_{sn}\lambda_s&=0\end{aligned}\right\} \tag{2-5}$$

但是，方程组（2-5）中未知量的个数大于方程的个数，故此时方程组必有非零解。〈证毕〉

定理2.1.2 线性空间V的维数等于V中基底向量的个数。

证明 设V的维数为n，则V中存在n个线性独立的向量

$$\boldsymbol{x}_1,\ \boldsymbol{x}_2,\ \cdots,\ \boldsymbol{x}_n \tag{2-6}$$

且V中任何多于n个向量必线性相关。设V的基底为

$$\boldsymbol{e}_1,\ \boldsymbol{e}_2,\ \cdots,\ \boldsymbol{e}_r \tag{2-7}$$

由上述引理，必有$n\leqslant r$。另一方面，对于每一个$e_i(i=1,2,\cdots,r)$，向量组

$$\boldsymbol{e}_i,\ \boldsymbol{x}_1,\ \boldsymbol{x}_2,\ \cdots,\ \boldsymbol{x}_n$$

都线性相关，即存在一组不全为零的数ξ_i，λ_1，λ_2，$\cdots$，λ_n使

$$\xi_i\boldsymbol{e}_i+\lambda_1\boldsymbol{x}_1+\lambda_2\boldsymbol{x}_2+\cdots+\lambda_n\boldsymbol{x}_n=\boldsymbol{0}$$

但$\xi_i\neq 0$，因此

$$\boldsymbol{e}_i=\sum_{k=1}^{n}\frac{\lambda_k}{\xi_i}\boldsymbol{x}_k$$

即向量组（2-7）中的每一个向量皆可表示为向量组（2-6）的线性组合。再由引理得，$r\leqslant n$。所以，$r=n$。　　〈证毕〉

虽然一个线性空间可以有许多基底，但是定理2.1.2指出，每一个基底所含基向量的个数是相同的，都等于该空间的维数。

例2.1.3　n维向量空间V_n中的向量组

$\boldsymbol{e}_1=(1,\ 0,\ \cdots,\ 0)$，$\boldsymbol{e}_2=(0,\ 1,\ \cdots,\ 0)$，$\cdots$，$\boldsymbol{e}_n=(0,\ 0,\ \cdots,\ 1)$是线性独立的。事实上，当

$$\lambda_1\boldsymbol{e}_1+\lambda_2\boldsymbol{e}_2+\cdots+\lambda_n\boldsymbol{e}_n=(\lambda_1,\ \lambda_2,\ \cdots,\ \lambda_n)=0$$

时，必有$\lambda_1=\lambda_2=\cdots=\lambda_n=0$

V_n中的任意元素$\boldsymbol{x}=(x_1,\ x_2,\ \cdots,\ x_n)$恒可表为$\boldsymbol{e}_1$，$\boldsymbol{e}_2$，$\cdots$，$\boldsymbol{e}_n$的线性组合：

$$\boldsymbol{x}=x_1\boldsymbol{e}_1+x_2\boldsymbol{e}_2+\cdots+x_n\boldsymbol{e}_n$$

因此，$\boldsymbol{e}_1$，$\boldsymbol{e}_2$，$\cdots$，$\boldsymbol{e}_n$是V_n的一个基底，而$(x_1,\ x_2,\ \cdots,\ x_n)$是向量$\boldsymbol{x}$在此基底下的坐标。

例2.1.4　考虑形如

$$[a_{ij}]=\begin{bmatrix} a_{11} & a_{12}\cdots a_{1n} \\ a_{21} & a_{22}\cdots a_{2n} \\ \vdots & \vdots\ \cdots\ \vdots \\ a_{n1} & a_{n2}\cdots a_{nn} \end{bmatrix}$$

的 $n\times n$ 矩阵所成的集合，其中阵元 $a_{ij}\in GF(2)$。不难验证，这一集合构成一个线性空间。在这个空间中取出除一个阵元为1而外，其余阵元全部为零的全体矩阵，它们便构成这个空间的基底。因此，这一线性空间是 n^2 维的。

下面讨论子空间的两种运算：**交与和**。

定理2.1.3 设 S 和 T 是线性空间 V 的两个子空间，则它们的交 $S\cap T$ 也是 V 的子空间。

证明 设 $\boldsymbol{x}$，$\boldsymbol{y}\in S\cap T$，即 $\boldsymbol{x}$，$\boldsymbol{y}\in S$ 且 $\boldsymbol{x}$，$\boldsymbol{y}\in T$，故 $\boldsymbol{x}+\boldsymbol{y}\in S$，$\boldsymbol{x}+\boldsymbol{y}\in T$，因而 $\boldsymbol{x}+\boldsymbol{y}\in S\cap T$。对于数量乘积可以类似地证明。所以，$S\cap T$ 是 V 的子空间。 〈证毕〉

显然，子空间的交适合交换律与结合律：

$$S\cap T=T\cap S$$

$$S\cap(T\cap U)=(S\cap T)\cap U$$

由于结合律成立，我们可以定义多个子空间的交，它也是子空间。

定义2.1.6 设 S 和 T 是线性空间 V 的子空间，称所有能表示成 $\boldsymbol{x}+\boldsymbol{y}$，而 $\boldsymbol{x}\in S$，$\boldsymbol{y}\in T$ 的向量组成的子集为 S 与 T 之和，并记为 $S+T$。

定理2.1.4 设 S 和 T 是线性空间 V 的两个子空间，则它们的和 $S+T$ 也是 V 的子空间。

证明 设 $\boldsymbol{x}$，$\boldsymbol{y}\in S+T$，即

$$\boldsymbol{x}=\boldsymbol{x}_1+\boldsymbol{x}_2,\quad \boldsymbol{x}_1\in S,\quad \boldsymbol{x}_2\in T$$

$$\boldsymbol{y}=\boldsymbol{y}_1+\boldsymbol{y}_2,\quad \boldsymbol{y}_1\in S,\quad \boldsymbol{y}_2\in T$$

于是，$\boldsymbol{x}+\boldsymbol{y}=(\boldsymbol{x}_1+\boldsymbol{y}_1)+(\boldsymbol{x}_2+\boldsymbol{y}_2)$

但是，

$$\boldsymbol{x}_1+\boldsymbol{y}_1\in S,\quad \boldsymbol{x}_2+\boldsymbol{y}_2\in T$$

因此，$\boldsymbol{x}+\boldsymbol{y}\in S+T$ 同样地，

$$\lambda\boldsymbol{x}=\lambda\boldsymbol{x}_1+\lambda\boldsymbol{x}_2\in S+T$$

可见，$S+T$ 是 V 的子空间。 〈证毕〉

与交的情形一样，子空间的和也满足交换律与结合律，并且可以定义多个子空间的和，它也是子空间。

定义2.1.7 向量组的一个部分组称为**极大线性无关组**，如果这个部分组线性无关，并且从这个向量组中任意添加一个向量后，所得的部分向量组都线性相关。我们称极大线性无关组中向量的个数为该向量组的**秩**。

定义2.1.8 设 x_1, x_2, …, x_r 和 y_1, y_2, …, y_s 是线性空间 V 中的两个向量组，且每一个向量组都可以用另一个向量组线性表出，则称这两个向量组是**等价的**。

定义2.1.9 设 x_1, x_2, …, x_r 是线性空间 V 中的一组向量。由它们所有可能的线性组合构成的集合是 V 的子空间，称为由 x_1, x_2, …, x_r 生成的子空间，并记为 $\langle x_1, x_2, \cdots, x_r\rangle$。

定理2.1.5 （1）两个向量组生成相同的子空间当且仅当这两个向量组等价。（2）$\langle x_1, x_2, \cdots, x_r\rangle$ 的维数等于向量组 x_1, x_2, …, x_r 的秩。

证明 （1）必要性：设 $\langle x_1, x_2, \cdots, x_r\rangle=\langle y_1, y_2, \cdots, y_s\rangle$，则每个向量 x_i 都可以用 y_1, y_2, …, y_s 线性表出。同理，每个向量 y_j 也可以用 x_1, x_2, …, x_r 线性表出。所以，这两个向量组等价。

充分性：设上述两个向量组等价，则对任意 $x\in\langle x_1, x_2, \cdots, x_r\rangle$，都有 $x\in\langle y_1, y_2, \cdots, y_s\rangle$。于是，$\langle x_1, x_2, \cdots, x_r\rangle\subseteq\langle y_1, y_2, \cdots, y_s\rangle$。同理可证 $\langle y_1, y_2, \cdots, y_s\rangle\subseteq\langle x_1, x_2, \cdots, x_r\rangle$。因此，$\langle x_1, x_2, \cdots, x_r\rangle=\langle y_1, y_2, \cdots, y_s\rangle$。

（2）设向量组 x_1, x_2, …, x_r 的秩为 s（$s\leqslant r$），且 x_1, x_2, …, x_s 是它的一个极大线性无关组。显然，x_1, x_2, …, x_r 与 x_1, x_2, …, x_s 等价，因此 $\langle x_1, x_2, \cdots, x_r\rangle=\langle x_1, x_2, \cdots, x_s\rangle$。可见，$x_1$, x_2, …, x_s 是 $\langle x_1, x_2, \cdots, x_r\rangle$ 的一组基底向量。由定理2.1.2，$\langle x_1, x_2, \cdots, x_r\rangle$ 的维数等于 s。

〈证毕〉

定理2.1.6 设 S 是 n 维线性空间 V_n 的一个 m 维子空间，e_1, e_2, …, e_m 是 S 的基底，则这组基底向量可以扩充为 V_n 的基底。换言之，在 V_n 中可以找到 $n-m$ 个向量 e_{m+1}, e_{m+2}, …, e_n，使

得e_1，e_2，…，e_n为V的基底。

证明 对维数差$n-m$用归纳法证之。当$n-m=0$时，定理显然成立。设$n-m=k$时，定理成立。我们讨论$n-m=k+1$的情形，

由于e_1，e_2，…，e_m线性无关，且不为V的基底，则存在$e_{m+1}\in V$，使e_{m+1}不能用e_1，e_2，…，e_m线性表出。于是，e_1，e_2，…，e_m，e_{m+1}线性无关，且由定理2.1.5，$\langle e_1, e_2, \cdots, e_m, e_{m+1}\rangle$是$m+1$维的子空间。因为$n-(m+1)=(n-m)-1=k+1-1=k$，由归纳法假设，$e_1$，$e_2$，…，$e_m$，$e_{m+1}$可以扩充为$V_n$的基底。〈证毕〉

下面的定理是很有用的。为了方便，我们用$\dim V$表示线性空间V的维数。

定理2.1.7 （维数公式） 设S和T是线性空间V的两个子空间，则

$$\dim S+\dim T=\dim(S+T)+\dim(S\cap T) \qquad (2\text{-}8)$$

证明 设$\dim S=k+i$，$\dim T=k+j$，$\dim(S\cap T)=k$，e_1，e_2，…，e_k是$S\cap T$的基底。由定理2.1.6，可以将它扩充成S的基底：

$$e_1,\ e_2,\ \cdots,\ e_k,\ x_1,\ \cdots,\ x_i$$

也可以扩充成T的基底：

$$e_1,\ e_2,\ \cdots,\ e_k,\ y_1,\ \cdots,\ y_j$$

如能证明

$$e_1,\ e_2,\ \cdots,\ e_k,\ x_1,\ \cdots,\ x_i,\ y_1,\ \cdots,\ y_j \qquad (2\text{-}9)$$

是$S+T$的基底，则$\dim(S+T)=k+i+j=\dim S+\dim T-\dim(S\cap T)$，因此定理得证。

由
$$S=\langle e_1,\ e_2,\ \cdots,\ e_k,\ x_1,\ \cdots,\ x_i\rangle$$
$$T=\langle e_1,\ e_2,\ \cdots,\ e_k,\ y_1,\ \cdots,\ y_j\rangle$$

显然有

$$S+T=\langle e_1,\ e_2,\ \cdots,\ e_k,\ x_1,\ \cdots,\ x_i,\ y_1,\ \cdots,\ y_j\rangle$$

剩下只需证明向量组（2-9）是线性无关的。设

$$\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_k e_k + \alpha_1 x_1 + \cdots + \alpha_l x_l$$
$$+ \beta_1 y_1 + \cdots + \beta_j y_j = 0$$

令
$$\alpha = \lambda_1 e_1 + \cdots + \lambda_k e_k + \alpha_1 x_1 + \cdots + \alpha_l x_l$$
$$= -\beta_1 y_1 - \cdots - \beta_j y_j$$

可见，$\alpha \in S$ 且$\alpha \in T$，因此$\alpha \in S \cap T$，即α可以用 e_1，…，e_k线性表出。令$\alpha = \gamma_1 e_1 + \cdots + \gamma_k e_k$，则

$$\gamma_1 e_1 + \cdots + \gamma_k e_k + \beta_1 y_1 + \cdots + \beta_j y_j = 0$$

因为e_1，…，e_k，y_1，…，y_j线性无关，故$\gamma_1 = \cdots = \gamma_k = \beta_1 = \cdots = \beta_j = 0$，所以$\alpha = 0$ 于是，

$$\lambda_1 e_1 + \cdots + \lambda_k e_k + \alpha_1 x_1 + \cdots + \alpha_l x_l = 0$$

因为e_1，…，e_k，x_1，…，x_l线性无关，故有 $\lambda_1 = \cdots = \lambda_k = \alpha_1 = \cdots = \alpha_l = 0$。因此，向量组（2-9）线性无关。 〈证毕〉

推论2.1.7.1 设 S 和 T 是 n 维线性空间V_n的两个子空间，且$\dim S + \dim T > n$，则$S \cap T$ 中必有非零向量。

证明 因为$\dim(S+T) + \dim(S \cap T) > n$，且 $\dim(S+T) \leqslant n$，所以$\dim(S \cap T) > 0$。 〈证毕〉

注意，如果线性空间V仅由零向量组成，则称V是 0 维的，并记作$\dim V = 0$

§2.2 线性分组码与生成矩阵

本节主要讨论线性分组码，下面给它下一个严格的定义。

定义2.2.1 $GF(2)$ 上的 n 维向量空间V_n的 k 维线性子空间V_k称为分组长为 n，信息位为 k 的**二元线性分组码**，简称为**二元线性码或二元（n，k）码**。

至于非线性码，那只是一些向量的集合。由于缺乏有力的工具，对非线性码的研究尚不成熟，我们只在第六章中予以简单介绍。除特别声明，在第六章以前提到的码，均指线性码而言。

上述定义很容易推广到一般情形。例如，三元（n，k）码指的是三元域$GF(3)$ 上 n 维向量空间V_n的 k 维子空间V_k。

显然，二元（n，k）码共有2^k个向量，而三元（n，k）

码则有3^k个码字。因为码是向量子空间，所以可出一组基底生成。这样就引出了生成矩阵的概念。

定义2.2.2 以（n，k）线性码V_k的基底向量

$$e_1=(v_{11}, v_{12}, \cdots, v_{1n})$$
$$e_2=(v_{21}, v_{22}, \cdots, v_{2n})$$
$$\cdots\cdots$$
$$e_k=(v_{k1}, v_{k2}, \cdots, v_{kn})$$

构成的矩阵

$$G=\begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{bmatrix}=\begin{bmatrix} v_{11} & v_{12}\cdots v_{1n} \\ v_{21} & v_{22}\cdots v_{2n} \\ \vdots & \vdots \cdots \vdots \\ v_{k1} & v_{k2}\cdots v_{kn} \end{bmatrix}$$

称为该（n，k）码的生成矩阵。

由于子空间可以有不只一个基底，因而一个（n，k）码也可以有多个生成矩阵。

例2.2.1 下述二元（6，3）码，其生成矩阵为

$$G=\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \tag{2-10}$$

这个码是$GF(2)$上的线性空间V_6的子空间V_3，它的三个基底是

$$e_1=(1\ 0\ 0\ 1\ 1\ 0)$$
$$e_2=(0\ 1\ 0\ 1\ 0\ 1)$$
$$e_3=(0\ 0\ 1\ 0\ 1\ 1)$$

e_1，e_2和e_3的全部线性组合就构成了该码的 8 个码字：

$$(0\ 0\ 0\ 0\ 0\ 0),\ (0\ 0\ 1\ 0\ 1\ 1),$$
$$(0\ 1\ 0\ 1\ 0\ 1),\ (0\ 1\ 1\ 1\ 1\ 0)$$
$$(1\ 0\ 0\ 1\ 1\ 0),\ (1\ 0\ 1\ 1\ 0\ 1),$$
$$(1\ 1\ 0\ 0\ 1\ 1),\ (1\ 1\ 1\ 0\ 0\ 0)$$

如果我们从这 8 个码字中另外选出一组基底向量

$$e_1' = (1\ 0\ 1\ 1\ 0\ 1)$$
$$e_2' = (1\ 1\ 0\ 0\ 1\ 1)$$
$$e_3' = (1\ 1\ 1\ 0\ 0\ 0)$$

就得到该码的另一个生成矩阵

$$G' = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \tag{2-11}$$

显然，$\langle e_1, e_2, e_3\rangle = \langle e_1', e_2', e_3'\rangle$

例2.2.2 考虑生成矩阵为

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix} \tag{2-12}$$

的三元（4，2）码，它是$GF(3)$上线性空间V_4的子空间V_2。由它的两个基底

$$e_1 = (1\ 0\ 1\ 1),\ e_2 = (0\ 1\ 2\ 1)$$

可以获得该码的全部$3^2 = 9$个码字

$$(0\ 0\ 0\ 0),\ (0\ 1\ 2\ 1),\ (0\ 2\ 1\ 2)$$
$$(1\ 0\ 1\ 1),\ (1\ 1\ 0\ 2),\ (1\ 2\ 2\ 0)$$
$$(2\ 0\ 2\ 2),\ (2\ 1\ 1\ 0),\ (2\ 2\ 0\ 1)$$

类似于例2.2.1，这个码也可以有其它的生成矩阵，例如

$$G' = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{pmatrix} \tag{2-13}$$

注意，$GF(3)$上的运算规则与$GF(2)$不同，在§1.4中已有说明。为方便读者，我们将$GF(3)$上的运算规则列表说明如下：

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

生成矩阵是编码时的重要工具，可以通过生成矩阵制订如下的编码规则。假如$m = (m_1, m_2, \cdots, m_k)$是一个消息组，则$m$

所对应的码向量是

$$mG=(m_1m_2\cdots m_k)\begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{bmatrix}=m_1e_1+m_2e_2+\cdots+m_ke_k$$

$$=m_1(v_{11}, v_{12}, \cdots, v_{1n})+m_2(v_{21}, v_{22}, \cdots, v_{2n})$$
$$+\cdots+m_k(v_{k1}, v_{k2}, \cdots, v_{kn})$$
$$=(m_1v_{11}+m_2v_{21}+\cdots+m_kv_{k1}, m_1v_{12}+m_2v_{22}$$
$$+\cdots+m_kv_{k2}, \cdots, m_1v_{1n}+m_2v_{2n}+\cdots+m_kv_{kn})$$

换言之，对应于消息组$m=(m_1, m_2, \cdots, m_k)$的码字是其生成矩阵$G$的诸行的线性组合。

因为线性码由其生成矩阵完全确定，所以编码器的存储量可以大大减少，它不必存储全部2^k个（指二元码）码向量而只需存储生成矩阵的k行。当然，编码器除存储器外，还需要有进行线性组合运算的运算器。对编码的基本要求是，编码设备越简单越好。综上所述，线性空间是符合编码需要的良好的数学结构。一般而言，线性码的编码是容易实现的。

适当地选取生成矩阵，还可以进一步简化编码设备。在例2.2.1中，二元（6，3）码的生成矩阵G较之于另一个生成矩阵G'有明显的特点

$$G=\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}=[I_3A]$$

其中I_3是3×3单位方阵，A是由剩余元素组成的矩阵。设$m=(m_1m_2m_3)$是消息组，则与其对应的码字为

$$(m_1m_2m_3)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$
$$=(m_1, m_2, m_3, m_1+m_2, m_1+m_3, m_2+m_3)$$

容易看出，码字的前3位与消息组完全相同，这是由生成矩阵的

特殊形状决定的。

定义2.2.3 生成矩阵形如

$$G=[I_kA]=\begin{bmatrix}1 & 0\cdots 0 & a_{11}\cdots a_{1n-k}\\ 0 & 1\cdots 0 & a_{21}\cdots a_{2n-k}\\ & \cdots & \cdots\\ 0 & 0\cdots 1 & a_{k1}\cdots a_{kn-k}\end{bmatrix}$$

的（n，k）线性码称作（n，k）**系统码**，其中I_k为$k\times k$方阵，A为$k\times(n-k)$矩阵。

（n，k）系统码的特点是，码字的前k位与对应的消息组相同，后$n-k$位是多余数字。

考虑消息组$\boldsymbol{m}=(m_1m_2\cdots m_k)$ 和它对应的码字

$\boldsymbol{u}=(u_1u_2\cdots u_n)=\boldsymbol{m}G=(m_1m_2\cdots m_k)[I_kA]$

显然有

$$\left.\begin{aligned}&u_i=m_i & i=1,2,\cdots,k\\ &u_{k+j}=a_{1j}m_1+a_{2j}m_2+\cdots+a_{kj}m_k & j=1,2,\cdots,n-k\end{aligned}\right\}\quad(2\text{-}14)$$

称式（2-14）为（n，k）系统码的**一致校验方程**。

为讨论线性分组码与系统码之间的关系作准备，我们引入矩阵的初等变换的概念。

所谓矩阵的**初等行变换**是指下列三种变换：

（a）交换矩阵的两行；

（b）以某一非零的数乘矩阵的某一行；

（c）以某一数乘矩阵的某一行再加到矩阵的另一行上去。

所谓**简化梯形矩阵**，是指具有下述性质的矩阵：

（a）每一个非零行的**首阵元**[1]均为1；

（b）含有此种首阵元为1的每一列的其余阵元均为零；

（c）每一零行均位于该矩阵的所有非零行的下方；

（d）假设矩阵有r个非零行，而第i行的首阵元所在之列为t_i（$i=1,2,\cdots,r$），则

$$t_1<t_2<\cdots<t_r$$

---

[1] 一个矩阵的任意非零行中第一个非零阵元叫作该行的首阵元。

定理2.2.1 任意矩阵都可以经过行初等变换化为简化梯形矩阵。

证明 设矩阵

$$A=\begin{pmatrix} a_{11} & \cdots a_{1t} & \cdots a_{1n} \\ a_{21} & \cdots a_{2t} & \cdots a_{2n} \\ \vdots & \cdots \vdots & \cdots \vdots \\ a_{i1} & \cdots a_{it} & \cdots a_{in} \\ \vdots & \cdots \vdots & \cdots \vdots \\ a_{m1} & \cdots a_{mt} & \cdots a_{mn} \end{pmatrix}$$

第一行的首阵元为a_{1t}，用a_{1t}^{-1}乘第一行便可使第一行的首阵元为1。然后，再将第一行乘以（$-a_{it}$）加到第i行上（$i\neq1$），便可使矩阵A化为

$$A'=\begin{bmatrix} 0 \cdots 1 \cdots a'_{1n} \\ a'_{21} \cdots 0 \cdots a'_{2n} \\ \cdots\cdots \\ a'_{m1} \cdots 0 \cdots a'_{mn} \end{bmatrix}$$

用同样的方法对下一个非零行进行这种变换，使该行的首阵元为1，该首阵元所在之列的其余元素为零。注意，对这个非零行进行上述变换时，并不改变前一非零行已经满足的性质。

经过有限次的上述行初等变换，就可以把矩阵A化为满足定义中条件（a）与（b）的矩阵。

最后，通过行之间的调换，可使A化为满足定义中条件(c)的矩阵，并使非零行的首阵元所在的列数按由小到大的次序排列，即使A化为满足条件（d）的矩阵。 《证毕》

例2.2.3 矩阵

$$\begin{bmatrix} 5 & 2 & 7 \\ -3 & 4 & 1 \\ -1 & -2 & -3 \end{bmatrix}$$

经过下述行初等变换可化为简化梯形矩阵，

$$\begin{pmatrix} 5 & 2 & 7 \\ -3 & 4 & 1 \\ -1 & -2 & -3 \end{pmatrix} \xrightarrow{\frac{1}{5}\times(1)} \begin{pmatrix} 1 & \frac{2}{5} & \frac{7}{5} \\ -3 & 4 & 1 \\ -1 & -2 & -3 \end{pmatrix}$$

$$\xrightarrow{3\times(1)+(2),\ (1)+(3)} \begin{pmatrix} 1 & \frac{2}{5} & \frac{7}{5} \\ 0 & \frac{26}{5} & \frac{26}{5} \\ 0 & \frac{-8}{5} & \frac{-8}{5} \end{pmatrix}$$

$$\xrightarrow{\frac{5}{26}\times(2)} \begin{pmatrix} 1 & \frac{2}{5} & \frac{7}{5} \\ 0 & 1 & 1 \\ 0 & \frac{-8}{5} & \frac{-8}{5} \end{pmatrix}$$

$$\xrightarrow{-\frac{2}{5}\times(2)+(1),\ \frac{8}{5}\times(2)+(3)} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

此处，$\frac{1}{5}\times(1)$表示将矩阵的第1行乘以$\frac{1}{5}$，$3\times(1)+(2)$表示以3乘矩阵的第1行再加到第2行上，余此类推。

对于二元矩阵，即阵元取自$GF(2)$的矩阵，行初等变换的第（b）条可以取消。同时，简化梯形矩阵条件（e）自然满足。

例2.2.4 二元矩阵

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

经过下述行初等变换后化为简化梯形矩阵：

$$\begin{bmatrix}1&0&0&1&0&1\\1&0&1&0&0&0\\1&0&0&1&1&0\end{bmatrix}\xrightarrow{(1)+(2),(1)+(3)}\begin{bmatrix}1&0&0&1&0&1\\0&0&1&1&0&1\\0&0&0&0&1&1\end{bmatrix}$$

如果交换所得矩阵的 2， 5 两列

$$\begin{pmatrix}1&0&0&1&0&1\\0&0&1&1&0&1\\0&0&0&0&1&1\end{pmatrix}\Longrightarrow\begin{pmatrix}1&0&0&1&0&1\\0&0&1&1&0&1\\0&1&0&0&0&1\end{pmatrix}$$

再交换最后一个矩阵的 2， 3 两列

$$\begin{pmatrix}1&0&0&1&0&1\\0&0&1&1&0&1\\0&1&0&0&0&1\end{pmatrix}\Longrightarrow\begin{pmatrix}1&0&0&1&0&1\\0&1&0&1&0&1\\0&0&1&0&0&1\end{pmatrix}=[I_3A]$$

最后得到系统矩阵，即系统码所对应的生成矩阵。

受这个例子启发，我们探讨系统码与线性分组码之间的关系。

定义2.2.4 两个线性码称为是等价的，如果一个线性码的生成矩阵可以通过行初等变换和列的置换化成另一个线性码的生成矩阵。

换言之，如果能够通过列的置换将一个线性码的全体码字变为另一个线性码的全体码字，则这两个线性码是彼此等价的。码的等价是编码理论中的一个重要概念，今后我们将看到，等价的码没有实质性的区别。

定理2.2.2 任意线性码都等价于一个系统码。

证明 设

$$G=\begin{pmatrix}v_{11}&v_{12}\cdots v_{1n}\\v_{21}&v_{22}\cdots v_{2n}\\\vdots&\vdots\;\cdots\;\vdots\\v_{k1}&v_{k2}\cdots v_{kn}\end{pmatrix}$$

是某一（n， k）码的生成矩阵，由定理2.2.1，经过行初等变换将G化为简化梯形矩阵。因为G的 k 个行向量线性无关并且构

成这一线性码的基底，所以G的秩[●]为k，记作$\mathrm{rank}G=k$。由矩阵代数可知，初等变换不改变矩阵的秩，因而$\mathrm{rank}G'=k$，即G'中没有全零行。于是，通过列的置换可以把G'化成系统矩阵$G''=[I_k A]$。〈证毕〉

对于系统码，编码设备可以进一步简化：编码器只需存储系统矩阵$[I_k A]$中A矩阵的阵元，共$k\times(n-k)$个数字a_{ij}。而对于线性码，则必须存储生成矩阵G中的全部阵元，共$k\times n$个数字v_{ij}。节约的存储量有k^2之多，当k很大时是很可观的。因此，工程实践上通常都采用系统码。

§2.3 一致校验矩阵

为了给线性码的理论以更好的直观说明，我们再引进一些几何概念。

定义2.3.1 设V_n为n维向量空间，且设$\boldsymbol{x}=(x_1, x_2, \cdots, x_n)\in V_n$，$\boldsymbol{y}=(y_1, y_2, \cdots, y_n)\in V_n$，则称

$$x_1y_1+x_2y_2+\cdots+x_ny_n$$

为向量$\boldsymbol{x}$，$\boldsymbol{y}$的内积，记为$\boldsymbol{x}\cdot\boldsymbol{y}$。特别当$\boldsymbol{x}\cdot\boldsymbol{y}=0$时，则称向量$\boldsymbol{x}$与$\boldsymbol{y}$正交，记为$\boldsymbol{x}\perp\boldsymbol{y}$。

不难证明，内积满足下述基本性质：

(1) $\boldsymbol{x}\cdot\boldsymbol{y}=\boldsymbol{y}\cdot\boldsymbol{x}$

(2) $(\lambda\boldsymbol{x})\cdot\boldsymbol{y}=\lambda(\boldsymbol{x}\cdot\boldsymbol{y})$，其中$\lambda$是数

(3) $(\boldsymbol{x}+\boldsymbol{y})\cdot\boldsymbol{z}=\boldsymbol{x}\cdot\boldsymbol{z}+\boldsymbol{y}\cdot\boldsymbol{z}$

注意，此处V_n可以定义在任意域上。特别当V_n是$GF(2)$上的n维向量空间时，内积定义为

$$\boldsymbol{x}\cdot\boldsymbol{y}=x_1y_1\oplus x_2y_2\oplus\cdots\oplus x_ny_n$$

此时，$\boldsymbol{x}\cdot\boldsymbol{y}=0$，即$\boldsymbol{x}\perp\boldsymbol{y}$意味着二元向量$\boldsymbol{x}$和$\boldsymbol{y}$中对应分量都是1的分量数为偶数。例如，$\boldsymbol{x}=(1\ 1\ 0\ 1\ 1)$，$\boldsymbol{y}=(0\ 1\ 0\ 0\ 1)$，它们的第2个分量和第5个分量都是1，因而$\boldsymbol{x}\cdot\boldsymbol{y}=0\oplus1\oplus0$

● 矩阵的秩定义为矩阵行向量组的秩。可以证明，矩阵的秩也等于矩阵列向量组的秩。

$\oplus 0 \oplus 1 = 0$。

设W是V_n的子空间，令U为与W中所有的向量都正交的V_n的全体向量所成的集合，即

$$U = \{\boldsymbol{u} \in V_n | \boldsymbol{u} \perp \boldsymbol{w}，对一切\boldsymbol{w} \in W\} \tag{2-15}$$

显然，集合U也是V_n的子空间。

定义2.3.2 设W是V_n的子空间，称式（2-15）所确定的子空间U为子空间W的**零化子空间**，记作$U = W^{\perp}$。

定理2.3.1 设W是n维向量空间V_n的k维子空间，则W的零化子空间U是$n-k$维的，并且U由W唯一确定。

证明 设

$$G = \begin{pmatrix} w_{11} & w_{12} \cdots w_{1n} \\ w_{21} & w_{22} \cdots w_{2n} \\ \vdots & \vdots \cdots \vdots \\ w_{k1} & w_{k2} \cdots w_{kn} \end{pmatrix} = \begin{pmatrix} \boldsymbol{w}_1 \\ \boldsymbol{w}_2 \\ \vdots \\ \boldsymbol{w}_k \end{pmatrix}$$

为子空间W的生成矩阵，则

$$\boldsymbol{u} \in U 当且仅当 \boldsymbol{u} \perp \boldsymbol{w}_i (i = 1, \cdots, k) \tag{2-16}$$

(2-16) 成立的必要性显然，今证充分性。设$\boldsymbol{u} \perp \boldsymbol{w}_i (i = 1, \cdots, k)$，对任意$\boldsymbol{w} \in W$，$\boldsymbol{w} = \lambda_1 \boldsymbol{w}_1 + \cdots + \lambda_k \boldsymbol{w}_k$，因此

$$\begin{aligned} \boldsymbol{u} \cdot \boldsymbol{w} &= \boldsymbol{u} \cdot (\lambda_1 \boldsymbol{w}_1 + \cdots + \lambda_k \boldsymbol{w}_k) \\ &= \lambda_1 (\boldsymbol{u} \cdot \boldsymbol{w}_1) + \cdots + \lambda_k (\boldsymbol{u} \cdot \boldsymbol{w}_k) = 0 \end{aligned}$$

即$\boldsymbol{u} \in U$。

由（2-16），求W的零化子空间相当于找出满足下列齐次线性方程组的解向量$\boldsymbol{u} = (u_1, u_2, \cdots, u_n)$的集合

$$\left.\begin{aligned} \boldsymbol{w}_1 \cdot \boldsymbol{u} &= w_{11} u_1 + w_{12} u_2 + \cdots + w_{1n} u_n = 0 \\ \boldsymbol{w}_2 \cdot \boldsymbol{u} &= w_{21} u_1 + w_{22} u_2 + \cdots + w_{2n} u_n = 0 \\ &\cdots \\ \boldsymbol{w}_k \cdot \boldsymbol{u} &= w_{k1} u_1 + w_{k2} u_2 + \cdots + w_{kn} u_n = 0 \end{aligned}\right\} \tag{2-17}$$

或简写为矩阵方程的形式

$$G\boldsymbol{u}' = \boldsymbol{O}$$

此处$\boldsymbol{u}'$表示$\boldsymbol{u}$的转置矩阵，而$\boldsymbol{O}$表示零矩阵。

不难证明，齐次线性方程组（2-17）的全体解向量构成线性空间，称为解空间，它是V_n的子空间。并且，由齐次线性方程组的结构定理可知，如果W是V_n的k维子空间，即W的生成矩阵G的秩为k，则方程组（2-17）的解空间为V_n的$n-k$维子空间，即$\dim U=n-k$。〈证毕〉

推论2.3.1.1 $W^{\perp\perp}=W$

证明 由$\perp$之定义，$W\subseteq W^{\perp\perp}$。根据定理2.3.1，$\dim W=\dim V_n-\dim W^{\perp}=\dim W^{\perp\perp}$。可见，$W^{\perp\perp}=W$。〈证毕〉

这个推论的含义是，U和W互为零化子空间，即若$U^{\perp}=W$，则$W^{\perp}=U^{\perp\perp}=U$。

以上所讨论的概念有一个很好的几何解释。例如，$\boldsymbol{xy}$平面可以视为该平面上由原点出发的全体向量所构成，它是3维向量空间V_3的2维子空间，其零化子空间为z轴上由坐标原点出发的一切向量所构成的1维子空间。

令

$$H=\begin{pmatrix} h_{11} & h_{12} & \cdots h_{1n} \\ h_{21} & h_{22} & \cdots h_{2n} \\ \vdots & \vdots & \cdots \vdots \\ h_{n-k1} & h_{n-k2} & \cdots h_{n-kn} \end{pmatrix}=\begin{pmatrix} \boldsymbol{h}_1 \\ \boldsymbol{h}_2 \\ \vdots \\ \boldsymbol{h}_{n-k} \end{pmatrix}$$

为W的零化子空间U的生成矩阵。于是

$$GH'=\begin{pmatrix} w_{11} & w_{12} & \cdots w_{1n} \\ w_{21} & w_{22} & \cdots w_{2n} \\ \vdots & \vdots & \cdots \vdots \\ w_{k1} & w_{k2} & \cdots w_{kn} \end{pmatrix}\begin{pmatrix} h_{11} & h_{21} & \cdots h_{n-k1} \\ h_{12} & h_{22} & \cdots h_{n-k2} \\ \vdots & \vdots & \cdots \vdots \\ h_{1n} & h_{2n} & \cdots h_{n-kn} \end{pmatrix}=\boldsymbol{O}$$

其中$\boldsymbol{O}$为$k\times(n-k)$零矩阵。

我们将零化子空间的概念应用到线性分组码上。先引入下述定义。

定义2.3.3 设C是$(n,\ k)$线性码，令$C^{\perp}=\{\boldsymbol{u}\in V_n|\boldsymbol{u}\perp\boldsymbol{v}$，对一切$\boldsymbol{v}\in C\}$，则称$C^{\perp}$是$C$的**对偶码**，或**正交码**。

由上面的讨论知道，$C^{\perp}$是C的零化子空间，因而是$n-k$

维的，即$C^{\perp}$是（n，$n-k$）线性码。

定义2.3.4 设C是（n，k）线性码，称$C^{\perp}$的生成矩阵H为C的**一致校验矩阵**。

因为C和$C^{\perp}$互为零化子空间，所以C的生成矩阵为G，一致校验矩阵为H，当且仅当$C^{\perp}$的生成矩阵为H，一致校验矩阵为G。

下面的定理告诉我们，一致校验矩阵H对于检验V_n中的向量是否为码向量起着关键作用。

定理2.3.2 设H是（n，k）码C的一致校验矩阵，$\boldsymbol{v}=(v_1, v_2, \cdots, v_n)$是$V_n$中的任意向量，则$\boldsymbol{v}\in C$当且仅当$\boldsymbol{v}H'=\boldsymbol{O}$。

证明 设$\boldsymbol{v}\in V_n$且满足$\boldsymbol{v}H'=\boldsymbol{O}$，则对于一切$\boldsymbol{u}\in C^{\perp}$恒有$\boldsymbol{u}\cdot\boldsymbol{v}=0$，即$\boldsymbol{v}\in C^{\perp\perp}=C$。反之，设$\boldsymbol{v}\in C$，则对一切$\boldsymbol{u}\in C^{\perp}$都有$\boldsymbol{u}\cdot\boldsymbol{v}=0$，从而自然有$\boldsymbol{v}H'=\boldsymbol{O}$。〈证毕〉

对于（n，k）线性码C，给定其生成矩阵G或一致校验矩阵H后，如何求H或G呢？下述定理关于系统码作出了回答。

定理2.3.3 设（n，k）系统码C的生成矩阵为$G=[I_kA]$，则C的一致校验矩阵为

$$H=[-A'I_{n-k}]$$

证明 设

$$G=[I_kA]=\begin{pmatrix} 1 & 0\cdots 0 & a_{11}\cdots a_{1n-k} \\ 0 & 1\cdots 0 & a_{21}\cdots a_{2n-k} \\ \vdots & \vdots\cdots\vdots & \vdots\cdots\vdots \\ 0 & 0\cdots 1 & a_{k1}\cdots a_{kn-k} \end{pmatrix}$$

则

$$H=[-A'I_{n-k}]=\begin{pmatrix} -a_{11} & -a_{21} & \cdots -a_{k1} & 1 & 0\cdots 0 \\ -a_{12} & -a_{22} & \cdots -a_{k2} & 0 & 1\cdots 0 \\ \vdots & \vdots & \cdots\ \vdots & \vdots & \vdots\cdots\vdots \\ -a_{1n-k} & -a_{2n-k} & \cdots -a_{kn-k} & 0 & 0\cdots 1 \end{pmatrix}$$

我们证明H是C的一致校验矩阵。

通过直接计算可以证明G和H中的行向量是彼此正交的。以G和H的第一个行向量为例，有$(1, 0, \cdots, 0, a_{11}, a_{12}, \cdots, a_{1n-k})\cdot(-a_{11}, -a_{21}, \cdots, -a_{k1}, 1, 0, \cdots, 0)=-a_{11}+a_{11}=0$。此外，$\operatorname{rank}G=k$，$\operatorname{rank}H=n-k$。（证毕）

例2.3.1 考虑例2.2.2中以

$$G=\begin{pmatrix}1 & 0 & 1 & 1\\ 0 & 1 & 2 & 1\end{pmatrix}=[I_2A]$$

为生成矩阵的三元（4，2）系统码。由定理2.3.3，可以立即写出它的一致校验矩阵

$$H=\begin{pmatrix}-1 & -2 & 1 & 0\\ -1 & -1 & 0 & 1\end{pmatrix}=\begin{pmatrix}2 & 1 & 1 & 0\\ 2 & 2 & 0 & 1\end{pmatrix}$$

因为$(2, 1, 1, 0)\cdot(1, 0, 1, 1)=2+1=3=0$

$(2, 1, 1, 0)\cdot(0, 1, 2, 1)=1+2=3=0$

$(2, 2, 0, 1)\cdot(1, 0, 1, 1)=2+1=3=0$

$(2, 2, 0, 1)\cdot(0, 1, 2, 1)=2+1=3=0$

所以这个例子证明了定理2.3.3的正确性。

对于二元（n，k）系统码，定理2.3.3中的$H=[-A'I_{n-k}]$可以简写成$H=[A'I_{n-k}]$。

§2.2中的（n，k）系统码的一致校验方程（2-14）也可以从一致校验矩阵求出。事实上，令$\boldsymbol{u}=(u_1u_2\cdots u_n)$为对应于消息组$\boldsymbol{m}=(m_1m_2\cdots m_k)$的码字，于是

$$u_i=m_i, \quad i=1, 2, \cdots, k$$

因为$\boldsymbol{u}H'=\boldsymbol{O}$，所以

$$-a_{11}u_1-\cdots-a_{k1}u_k+u_{k+1}=0$$

$$\cdots$$

$$-a_{1n-k}u_1-\cdots-a_{kn-k}u_k+u_n=0$$

于是，当$j=1, 2, \cdots, n-k$时

$$\begin{aligned}u_{k+j}&=a_{1j}u_1+a_{2j}u_2+\cdots+a_{kj}u_k\\&=a_{1j}m_1+a_{2j}m_2+\cdots+a_{kj}m_k\end{aligned}$$

此即一致校验方程（2-14）。当且仅当$u=(u_1u_2\cdots u_n)$满足这个一致校验方程时，u才是系统码中的码字。这正是一致校验方程名称的由来。

由此可见，线性码可由其生成矩阵或一致校验矩阵完全确定。讨论编码问题时，常常用到生成矩阵，而讨论译码问题时，则常常利用一致校验矩阵。两者相辅相成。

最后，我们证明一个有用的公式。

定理2.3.4 设S和T是线性空间V的两个子空间，则

$$(S^{\perp}\cap T^{\perp})=(S+T)^{\perp}$$

证明 设$x\in S^{\perp}\cap T^{\perp}$，对任意$y=y_1+y_2\in S+T$，其中$y_1\in S$，$y_2\in T$，恒有$x\cdot y=x\cdot y_1+x\cdot y_2=0+0=0$，故$x\in(S+T)^{\perp}$。因此，$(S^{\perp}\cap T^{\perp})\subseteq(S+T)^{\perp}$。反之，设$x\in(S+T)^{\perp}$，因$\mathbf{0}\in T$，故对任何$y_1\in S$恒有$x\cdot y_1=x\cdot(y_1+\mathbf{0})=0$，因而$x\in S^{\perp}$。同理，$x\in T^{\perp}$。于是，$x\in S^{\perp}\cap T^{\perp}$，即$(S+T)^{\perp}\subseteq(S^{\perp}\cap T^{\perp})$。〈证毕〉

§2.4 线性码的译码

一般而言，编码是比较容易实现的，困难的任务在于译码。编码理论的一个中心课题就是设计有效的译码方案。译码方案大体上可以分为两种，一种是用于特定的码或码类的专用的译码方法；另一种是可用于任意码的一般译码方法。通常，前者比后者更为快捷和简便。这一节所介绍的是伴随式译码的一般译码方案，也可以作为衡量其它译码方案的标准。换言之，在采用一种新的译码方法之前，最好先和伴随式译码方案进行比较。

首先引入陪集的概念。

定义2.4.1 设C是(n,k)线性码，$a\in V_n$，称集合$\{a+c|c\in C\}$为由a确定的C的**陪集**，记为$a+C$。

显然，上述陪集包含元素a。一般，对于任意$u\in V_n$，都有某个C的陪集包含u。例如，$u+C$包含u。不难看出，若$a\in C$，则$a+C=C$。因此，C本身就是一个陪集。此外，若$b\in a+$

C，即$\boldsymbol{b}=\boldsymbol{a}+\boldsymbol{c}$，其中$\boldsymbol{c}\in C$，于是，$\boldsymbol{b}+C=(\boldsymbol{a}+\boldsymbol{c})+C=\boldsymbol{a}+(\boldsymbol{c}+C)=\boldsymbol{a}+C$。这表明陪集$\boldsymbol{a}+C$可以由其中任一元素唯一地确定。

陪集还有下述重要的性质。

定理2.4.1 同一个陪集中任何两个向量均不相同；不同的陪集之间彼此不相交。

证明 设$\boldsymbol{a}_1$，$\boldsymbol{a}_2\in\boldsymbol{a}+C$，则$\boldsymbol{a}_1=\boldsymbol{a}+\boldsymbol{c}_1$，$\boldsymbol{a}_2=\boldsymbol{a}+\boldsymbol{c}_2$，其中$\boldsymbol{c}_1$，$\boldsymbol{c}_2\in C$，且$\boldsymbol{c}_1\neq\boldsymbol{c}_2$。如果$\boldsymbol{a}_1=\boldsymbol{a}_2$，就有$\boldsymbol{a}+\boldsymbol{c}_1=\boldsymbol{a}+\boldsymbol{c}_2$，因此$\boldsymbol{c}_1=\boldsymbol{c}_2$，产生矛盾。

其次，设$\boldsymbol{a}+C\neq\boldsymbol{b}+C$。假定$\boldsymbol{u}\in\boldsymbol{a}+C\cap\boldsymbol{b}+C$，则$\boldsymbol{u}=\boldsymbol{a}+\boldsymbol{c}_1=\boldsymbol{b}+\boldsymbol{c}_2$，其中$\boldsymbol{c}_1$，$\boldsymbol{c}_2\in C$。设$\boldsymbol{v}$是$\boldsymbol{a}+C$中的任一向量，则$\boldsymbol{v}=\boldsymbol{a}+\boldsymbol{c}_3=\boldsymbol{b}+\boldsymbol{c}_2-\boldsymbol{c}_1+\boldsymbol{c}_3\in\boldsymbol{b}+C$。于是，$\boldsymbol{a}+C\subseteq\boldsymbol{b}+C$。同理可证$\boldsymbol{b}+C\subseteq\boldsymbol{a}+C$。因而$\boldsymbol{a}+C=\boldsymbol{b}+C$，与假定矛盾。

〈证毕〉

由这一定理可知，每一个陪集$\boldsymbol{a}+C$中向量的个数都是一样的，即为C中所含向量的个数。如果C是$GF(q)$上的(n, k)码，则有$|C|=q^k$。同时，V_n中每一向量$\boldsymbol{a}$均含在且仅含在C的一个陪集中，即含于$\boldsymbol{a}+C$中。因此，V_n是C的所有陪集的并集。由此可得，V_n中共有q^{n-k}个C的陪集。特别，当C是二元(n, k)码时，$|C|=2^k$，且C有2^{n-k}个陪集。注意，C的全部陪集中，除C本身外都不构成子空间，因为这些陪集中都没有零向量。

向量的重量是编码理论中的一个重要概念，其定义为

定义2.4.2 设$\boldsymbol{x}\in V_n$，称向量$\boldsymbol{x}=(x_1, x_2, \cdots, x_n)$中坐标不为零的个数为该向量的**汉明重量**，简称**重量**，记为$w(\boldsymbol{x})$。

注意，定义1.3.1中的向量实际上可以是$GF(q)$上的向量。不难看出，距离和重量之间有着密切的联系

$$d(\boldsymbol{x}, \boldsymbol{y})=w(\boldsymbol{x}-\boldsymbol{y})$$

现在考虑接收向量$\boldsymbol{r}=(r_1, r_2, \cdots, r_n)$，将它视为发送码向量$\boldsymbol{v}$与错误向量$\boldsymbol{e}=(e_1, e_2, \cdots, e_n)$之和。因而$\boldsymbol{e}=\boldsymbol{r}-\boldsymbol{v}=(r_1-v_1, \cdots, r_n-v_n)$，其中$e_i=0$当且仅当$r_i=v_i$。错误向量$\boldsymbol{e}$也称

为错误格式。

接收向量 r 属于 C 的某个陪集，如果在该陪集中选取一个重量最小的向量 e，并将 r 译码为 $v=r-e$，则 v 将是 C 中最接近 r 的向量。当然，一个陪集中重量最小的向量，称为**陪集首**，可能不只一个。这时，我们可以随机地选取其中一个。

译码时，我们可以将 V_n 中的全体向量排列成表的形式，其中每一行都是 C 的一个陪集，方法如下。第一行是 C 本身，其中第一列是零向量。其余各行（即其它陪集）中的第一列都是陪集首，剩余的列都是该陪集首与第一行中位于相应列码字的和。称按上述方式排列的向量表为码 C 的**标准阵列**。

例2.4.1 考虑生成矩阵为

$$G=\begin{pmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 1 & 1\end{pmatrix}$$

的二元（4，2）系统码 C，其一致校验矩阵为

$$H=\begin{pmatrix}0 & 1 & 1 & 0\\ 1 & 1 & 0 & 1\end{pmatrix}$$

标准阵列中的第一行是 4 个码向量，其中零向量排在左边（见表 2-1，暂不理会伴随式那一列）。然后在 V_4 中剩下的 12 个向量里面，挑选一个重量最小的向量，例如（1 0 0 0），作为第二行的陪集首。将（1 0 0 0）与第一行中所有的码字相加，就得到第二行。接着，在剩下的 8 个向量中选取（0 1 0 0）为第三行的陪集首，等等。在我们的例子中，陪集首重量皆为 1 的向量，但对

表 2-1

伴随式	陪　集　首				注　释
0 0	0 0 0 0	1 0 0 1	0 1 1 1	1 1 1 0	C
0 1	1 0 0 0	0 0 0 1	1 1 1 1	0 1 1 0	(1 0 0 0)+C
1 1	0 1 0 0	1 1 0 1	0 0 1 1	1 0 1 0	(0 1 0 0)+C
1 0	0 0 1 0	1 0 1 1	0 1 0 1	1 1 0 0	(0 0 1 0)+C

于其它的码，陪集首的重量可能为2，3，4，……。

假定接收向量$r=(1\ 0\ 1\ 0)$，我们在表2-1的第3行第4列中找到了它，就可以把r译成位于第4列的码字$v=(1\ 1\ 1\ 0)$。显然，位于第3行的陪集首$(0\ 1\ 0\ 0)$是错误向量e，表示信道第2位有错。由此可见，译码正确与否的关键在于信道错误向量是否是陪集首。因为我们将r译为与它最接近的码向量v，所以符合最大似然译码准则。

当C为码长100的二元码时，C的标准阵列由2^{100}个阵元组成，译码器必须存储它们，译码时还必须从中搜索接收向量r，这在工程实践上是很难实现的。伴随式译码方案对此作出了改进。

定义2.4.3 设H为(n, k)码C的一致校验矩阵，r是V_n中的任意向量，称$s=rH^t$为r的伴随式。

显然，伴随式s是有$(n-k)$个坐标的行向量。r是C中的向量当且仅当$s=0$。

伴随式具有下列重要性质。

定理2.4.2 V_n中的两个向量x和y属于C的同一个陪集当且仅当x和y具有相同的伴随式。

证明 设x，$y\in a+C$，即$x=a+c_1$，$y=a+c_2$，c_1，$c_2\in C$。于是，

$$xH^t=(a+c_1)H^t=aH^t+c_1H^t=aH^t$$
$$yH^t=(a+c_2)H^t=aH^t+c_2H^t=aH^t$$

此处H是(n, k)码C的一致校验矩阵。由此得$xH^t=yH^t$，即x和y有相同的伴随式。

反之，设$xH^t=yH^t$，则$(x-y)H^t=0$，因此$(x-y)$是C中的码向量。记作$x-y=c$，$c\in C$，则$x=y+c$，即x和y属于C的同一个陪集。〈证毕〉

这个定理说明，$GF(q)$上的(n, k)码C的一个陪集的全部q^k个向量具有相同的伴随式，并且不同陪集的伴随式亦不相同。因为C共有q^{n-k}个不同的陪集，所以有q^{n-k}个不同的伴随式。但是，伴随式s是有$(n-k)$个坐标的行向量，因此，

它所有可能的组合方式是 q^{n-k} 种。由此可见，全部 q^{n-k} 个伴随式都将作为 V_n 中某些向量的伴随式出现，亦即标准阵列中的 q^{n-k} 个陪集与 q^{n-k} 个伴随式之间存在一一对应的关系。

继续考察例 2.4.1 中的 2 元（4，2）系统码 C，与 C 的标准阵列中的 4 个陪集首（0 0 0 0）、（1 0 0 0）、（0 1 0 0）和（0 0 1 0）相对应的 4 个伴随式分别为（0 0），（0 1），（1 1）和（1 0），如表 2-1 所示。当接收向量 $r=(1\ 0\ 1\ 0)$ 时，计算出它的伴随式为

$$(1\ 0\ 1\ 0)\begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}=(1\ 1)$$

与其对应的陪集首是（0 1 0 0），因而可以将 r 译为（1 0 1 0）+（0 1 0 0）=（1 1 1 0）。

现在，我们可以给出伴随式译码方法了。

第一步，计算接收向量 r 的伴随式 rH^t；

第二步，求出伴随式等于 rH^t 的陪集首 e；

第三步，将 r 译为 $v=r-e$

显然，这一方法符合最大似然译码准则。

按照这个方法译码，不必排出 C 的标准阵列，只需排出伴随式和陪集首这两列就够了。实际作法是，将零向量作为码 C 的陪集首与伴随式，然后选取重量为 1 的向量作陪集首，并计算其伴随式。每当求出一个新的伴随式，就得到一个新的陪集首。如果重量为 1 的向量已经用完，而陪集首的个数还不够时，就在重量为 2 的向量中继续寻找新的陪集首。如此继续下去，只要得到一个新的伴随式，就将它和与之对应的重量为 i 的陪集首排在一起，构成表中的一个新行。当重量为 i 的向量用完以后，就考察重量为 $i+1$ 的向量，直到获得 q^{n-k} 个伴随式时为止。

伴随式译码方法适用于任意（n，k）线性码，并且大大降低了译码器的存储量。以二元（100，60）码为例，我们只需存

储 2^{40} 个陪集首和伴随式，较之存储 2^{100} 个标准阵列的阵元是很大的改进。此外，搜索 2^{40} 个伴随式也比搜索 2^{100} 个向量简捷得多。伴随式译码方法是目前所知的最好的通用译码方法，如果要进一步改进，就必须对线性码加以更强的限制。然而，限制越强，译码方法的专用程度也就越高。

下面，我们介绍最佳码的概念。为此，先给出下述定义。

定义2.4.4 称陪集首的重量为它所在的**陪集重量**。码的**陪集重量分布**指数集 $\{a_i\}$，其中 a_i 是重量为 i 的陪集个数。

对于给定的 n 和 k，选择 V_n 的不同的 k 维子空间为（n，k）码时，其陪集的总重量 $\sum_{i=0}^{n} a_i i$ 一般来说也随之不同。因此，为了保证正确译码的概率最大，应当选择**使陪集总重量最小的** k 维子空间作为（n，k）码。我们称这种 k 维子空间为**最佳码**。

例如，例 2.4.1 中的二元（4，2）码 C 的陪集重量分布为 $a_0=1$，$a_1=3$，故 $\sum_{i=0}^{n} a_i i=3$，因此 C 是最佳码。若取

$$G=\begin{pmatrix}1 & 1 & 0 & 0\\0 & 0 & 1 & 1\end{pmatrix}$$

为生成矩阵，则相应的二元（4，2）码的标准阵列为

0 0 0 0	1 1 0 0	0 0 1 1	1 1 1 1
1 0 0 0	0 1 0 0	1 0 1 1	0 1 1 1
0 0 1 0	1 1 1 0	0 0 0 1	1 1 0 1
0 1 0 1	1 0 0 1	0 1 1 0	1 0 1 0

它的陪集重总量为 4，因而不是最佳码。

最后，我们讨论伴随式译码方法的误码率问题。

我们已经说过，当采用伴随式译码方法时，译码器总是选择某个陪集首作为错误向量。因此，译码正确与否取决于陪集首是否为真实的错误向量。于是，在二元对称信道中，

$$p_e = p(e \neq \text{陪集首}) = 1 - \sum_{i=0}^{n} a_i p^i q^{n-i}$$

其中 a_i 是码 C 的陪集重量分布。

对于例 2.4.1 中的二元（4，2）码，$a_0 = 1$，$a_1 = 3$。设 $q = 0.99$，则

$$p_e = 1 - q^4 - 3pq^3 \approx 0.0103$$

如果码的最小距离 $d = 2t + 1$ 或 $2t + 2$，则由定理 1.3.2，该码的纠错能力为 t。因此，每一个重量 $\leqslant t$ 的错误向量都是陪集首，即

$$a_i = \binom{n}{i} \qquad i = 0, 1, \cdots, t$$

但是，当 $i > t$ 时，a_i 的计算就变得十分困难了，只有少数码例外。例如，

定义2.4.5 最小距离为 d 的码 C 称作**完备码**，如果 $a_i = 0$，对一切 $i > t = [(d-1)/2]$。

不难看出，t 一纠错完备码可以纠正所有重量 $\leqslant t$ 的错误，而不能纠正任何重量 $> t$ 的错误。今后，我们将进一步讨论完备码。

定义2.4.6 最小距离为 d 的码 C 称作**拟完备码**，如果 $a_i = 0$，对一切 $i > t + 1$，其中 $t = [(d-1)/2]$。

因此，t 一纠错拟完备码可以纠正所有重量 $\leqslant t$ 的错误，某些重量 $= t + 1$ 的错误，但不能纠正任何重量 $> t + 1$ 的错误。最后，我们举一个拟完备码的例子结束本节。

例2.4.2 考虑例 2.2.1 中的二元（6，3）码 C，已知 C 的最小距离 $d(C) = 3$。因此 C 的陪集重量分布为 $a_0 = 1$，$a_1 = \binom{6}{1} = 6$。还剩下一个陪集首，其重量如何就不清楚了，即当 $i > t\ (= 1)$ 时，没有公式可以方便地计算 a_i。但对于这个特例，我们还是可以较快地推断出 $a_2 = 1$，因为码字中共有 4 个重量为

3的向量，6个重量为1的陪集首和它们相加后消去了12个重量为2的向量，最后尚剩余$\binom{6}{2}-12=3$个重量为2的向量可以入选为陪集首。因此，C是单纠错拟完备码。

仍设$q=0.99$，则有

$$p_e=1-q^6-6pq^5-p^2q^4\approx 0.00136$$

§2.5 线性码的一般性质

本节将要介绍线性码的若干重要性质。

平行于最小（汉明）距离，有最小（汉明）重量的概念。

定义2.5.1 一个分组码C的最小（汉明）重量是指

$$d(C)\triangleq \min_{\substack{c\in C\\ c\neq 0}} w(\boldsymbol{c})$$

下面的定理说明了线性码的优越性。

定理2.5.1 线性码的最小距离等于最小重量。

证明 设C为线性码，$\boldsymbol{x}$，$\boldsymbol{y}\in C$，则$\boldsymbol{x}-\boldsymbol{y}\in C$。因为$C$的最小距离

$$\begin{aligned} d(C)&=\min d(\boldsymbol{x},\ \boldsymbol{y})\\ &=\min w(\boldsymbol{x}-\boldsymbol{y}),\ \boldsymbol{x},\ \boldsymbol{y}\in C,\ \boldsymbol{x}\neq \boldsymbol{y} \end{aligned}$$

所以，

$$d(C)=\min_{\substack{c\in C\\ c\neq 0}} w(\boldsymbol{c})$$

〈证毕〉

因此，求线性码的最小距离就变成求最小重量的问题。显然，后者要容易得多。今后，将最小重量为d的$(n,\ k)$线性码记为$(n,\ k,\ d)$码。码长n，维数k和最小重量d是线性码最重要的三个参数。

设C为$(n,\ k,\ d)$码，考虑以码点为中心，以$t=[(d-1)/2]$为半径的码球。称t为球包半径。

定理2.5.2 球包半径 t 具有下述性质：

（1） $t=\max\{s\mid$半径为 s 的码球互不相交$\}$；

（2） $t=\max\{s\mid$任意重量$\leqslant s$的向量都是陪集首$\}$。

证明 （1）定理1.3.2已经证明半径为 t 的码球互不相交。现在只需证明半径为 $t+1$ 的码球一定相交。

设$\boldsymbol{x}\in C$且$w(\boldsymbol{x})=d$。若d为偶数，令向量$\boldsymbol{y}$的重量为$d/2$，且$\boldsymbol{y}$的全部$d/2$个非零坐标都对应于$\boldsymbol{x}$的非零坐标。由于$d(\boldsymbol{y},\boldsymbol{x})=d(\boldsymbol{y},\boldsymbol{0})=d/2=t+1$，故有$\boldsymbol{y}\in S_{t+1}(\boldsymbol{x})\cap S_{t+1}(\boldsymbol{0})$。若$d$为奇数，令向量$\boldsymbol{y}$的重量为$(d+1)/2$，且$\boldsymbol{y}$的全部非零分量都对应于$\boldsymbol{x}$的非零分量。因为$d(\boldsymbol{y},\boldsymbol{x})=d-(d+1)/2=(d-1)/2=t$，且$d(\boldsymbol{y},\boldsymbol{0})=(d+1)/2=t+1$。所以，$\boldsymbol{y}\in S_{t+1}(\boldsymbol{x})\cap S_{t+1}(\boldsymbol{0})$。

（2）我们知道，任何重量$\leqslant t$的向量都是陪集首，剩下来只需证明有一个重量为$t+1$的向量不是陪集首。若d为偶数，设$\boldsymbol{x}\in C$且$w(\boldsymbol{x})=d=2t+2$。令$w(\boldsymbol{y})=t+1$，且$\boldsymbol{y}$的全部$t+1$个非零分量都对应于$\boldsymbol{x}$的非零分量。于是，$\boldsymbol{z}=\boldsymbol{x}-\boldsymbol{y}$与$-\boldsymbol{y}$属于$C$的同一个陪集，且$w(\boldsymbol{z})=w(-\boldsymbol{y})=t+1$。因此，$\boldsymbol{z}$和$-\boldsymbol{y}$中至少有一个不是陪集首。若$d$为奇数，设$\boldsymbol{x}\in C$且$w(\boldsymbol{x})=d=2t+1$。令$w(\boldsymbol{y})=t+1$，且$\boldsymbol{y}$的所有非零分量都对应于$\boldsymbol{x}$的非零分量。因此，$\boldsymbol{z}=\boldsymbol{x}-\boldsymbol{y}$与$-\boldsymbol{y}$属于$C$的同一个陪集。但是，$w(\boldsymbol{z})=t$，$w(-\boldsymbol{y})=t+1$。所以，$-\boldsymbol{y}$不可能是陪集首。 〈证毕〉

如果以s为半径的码球包含V_n中的全部向量，就称这些码球**覆盖空间**V_n。所谓码C的**覆盖半径**指的是

$$r=\min\{s\mid \text{半径为 } s \text{ 的码球覆盖整个空间 } V_n\}$$

下述定理揭示了覆盖半径与陪集重量之间的联系。

定理2.5.3 覆盖半径r是具有最大重量的陪集的重量。

证明 设a是具有最大重量的陪集首的重量，我们分两步证明定理。第一步，先证半径为a的码球覆盖空间V_n。如果不然，则有一个向量$\boldsymbol{y}\in V_n$，使$d(\boldsymbol{y},\boldsymbol{c})>a$，对一切$\boldsymbol{c}\in C$。但是，

y必属于C的某个陪集，设其陪集首为x。于是，$y-x=c_1$，$c_1\in C$。因此，$d(y,\ c_1)=d(x+c_1,\ c_1)=w(x)\leqslant a$，产生矛盾。所以，半径为$a$的码球覆盖$V_n$。可见，$r\leqslant a$。第二步，我们证明$C$中任意陪集的重量都$\leqslant r$。假设不然，设$x$是陪集首，且$w(x)>r$，则对一切$c\in C$，都有$d(c,\ x)=w(x-c)>r$。否则，$x$与$x-c$属于同一个陪集，且$w(x-c)\leqslant r<w(x)$，与$x$为陪集首的假定矛盾。因此，任意以$r$为半径的码球都不包含$x$，与覆盖半径$r$的定义冲突。因此，$a\leqslant r$。由此得，$r=a$。 〈证毕〉

定理 2.5.3 使我们可以用覆盖半径的语言重新定义完备码和拟完备码。

定义2.5.2 设r，t分别是$(n,\ k,\ d)$码C的覆盖半径和球包半径。称C是**t—纠错完备码**，如果$r=t$。称C是**t—纠错拟完备码**，如果$r=t+1$。

显然，这个定义与前面的两个定义 2.4.5 和 2.4.6 是完全等价的。

例2.5.1 继续考察例 2.2.1 和例 2.4.2 中的二元$(6,\ 3)$拟完备码C，其标准阵列为

000000	001011	010101	100110	111000	011110	101101	110011
100000	101011	110101	000110	011000	111110	001101	010011
010000	011011	000101	110110	101000	001110	111101	100011
001000	000011	011101	101110	110000	010110	100101	111011
000100	001111	010001	100010	111100	011010	101001	110111
000010	001001	010111	100100	111010	011100	101111	110001
000001	001010	010100	100111	111001	011111	101100	110010
001100	000111	011001	101010	110100	010010	100001	111111

由标准阵列可见，$r=2$，$t=[(3-1)/2]=1$。我们计算在半径为$t=1$的码球内包含V_6中向量的个数。显然，$S_1(\mathbf{0})$中含有零向量和 6 个重量为 1 的向量，共计 7 个向量。其次，对任意$x\in C$，$S_1(x)$中也包含 7 个向量，因为这个码球内的任意向量都可以由x与$S_1(\mathbf{0})$中的向量相加而得到。但C中共有$2^3=8$个向量，故在这些码球内共有$7\times 8=56$个V_6中的

向量。因此，V_6中尚有$2^6-56=8$个向量在这些码球之外。显然，这8个向量属于C的标准阵列中的最后一行。此外，设$\boldsymbol{x}\in C$，则$S_1(\boldsymbol{x})$中包含的向量即为C的标准阵列中$\boldsymbol{x}$所在列的前7个向量。

因为C的重量分布为$a_0=1$，$a_3=4$，$a_4=3$，其中a_i表示C中重量为i的向量个数。通过更仔细的计算可得，(i) 若$w(\boldsymbol{x})=3$，则$S_1(\boldsymbol{x})$中向量的重量分布是$a_2=a_4=3$，$a_3=1$；(ii) 若$w(\boldsymbol{y})=4$，则$S_1(\boldsymbol{y})$中向量的重量分布为$a_3=4$，$a_4=1$，$a_5=2$；(iii) $S_1(\mathbf{0})$中向量的重量分布为$a_0=1$，$a_1=6$。因此，半径为1的码球内的向量的重量分布为$a_0=1$，$a_1=6$，$a_2=12$，$a_3=16$，$a_4=15$，$a_5=6$，$a_6=0$。但是，V_6的重量分布为$a_0=a_6=1$，$a_1=a_5=6$，$a_2=a_4=15$，$a_3=20$。可见，这些码球外的向量的重量分布是$a_2=3$，$a_3=4$，$a_6=1$。这就是C的标准阵列中最后一行的重量分布。

顺便指出，由C的标准阵列可见，C是最佳码。事实上，由完备码和拟完备码的定义立即可得：**完备码和拟完备码一定是最佳码。**

下述定理是很有用的。有了它，我们可以通过C的一致校验矩阵提取有关最小重量$d(C)$的信息。

定理2.5.4 设$\boldsymbol{u}$为C中重量为m的向量，则在C的一致校验矩阵H的m列中存在一个线性相关关系。反之，对于H的m列中任何一个线性相关关系，都对应一个C中重量为m的码字。

证明 向量$\boldsymbol{u}=(u_1, u_2, \cdots, u_n)\in C$当且仅当

$$\boldsymbol{u}H'=\mathbf{0}$$

或者，H的第i个列向量记为$\boldsymbol{h}_i$，则有

$$u_1\boldsymbol{h}_1+u_2\boldsymbol{h}_2+\cdots+u_n\boldsymbol{h}_n=\mathbf{0}$$

因此，

$$u_{i_1}\boldsymbol{h}_{i_1}+u_{i_2}\boldsymbol{h}_{i_2}+\cdots+u_{i_m}\boldsymbol{h}_{i_m}=\mathbf{0} \tag{2-18}$$

其中，$u_{i_k}\neq 0$，$k=1, 2, \cdots, m$。式(2-18)即H中m列的一个线性相关关系。

反之，若式（2-18）成立，显然C中有一个向量$\boldsymbol{u}=(u_1, u_2, \cdots, u_n)$与之对应，其中$w(\boldsymbol{u})=m$。　　　　〈证毕〉

推论2.5.4.1　C的最小重量为d当且仅当$d=\max\{m|C$的一致校验矩阵H的任意$m-1$列都线性无关$\}$。

证明　由定理2.5.4可得。　　　　〈证毕〉

由此可见，H中没有全零列当且仅当C中没有重量为1的向量。对于二元码，H中的列全不相同意味着H中任意2列之和皆不为零。因此，任何线性相关关系都至少包含3列，即$d\geqslant 3$。对于q元码C，$d\geqslant 3$则意味着H中的任一列都不是其它列的倍数。

注意推论中的条件与矩阵的秩的定义之间的区别。对于一个秩为m的矩阵，有一组m个列向量线性无关就够了，并不要求任意m列都线性无关。

定义2.5.3　设G为(n, k)码C的生成矩阵，称G中任意k个线性无关的列为C的**信息组**。

定理2.5.5　设G为(n, k, d)码C的生成矩阵，则G的任意$n-d+1$列都包含一个信息组。此外，d为具有这种性质的数中最大者。

证明　设G中有$n-d+1$个列，它的列坐标为集合S，其中任意k列都线性相关。考虑G的部分矩阵A，A的列由G中具有列坐标S的列组成。显然，A是$k\times(n-d+1)$矩阵，且$\mathrm{rank}A<k$。因此，A的诸行$\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_k$线性相关，即

$$\lambda_1\boldsymbol{a}_1+\lambda_2\boldsymbol{a}_2+\cdots+\lambda_k\boldsymbol{a}_k=\boldsymbol{0}$$

其中λ_i不全为零。令G的行向量为$\boldsymbol{g}_1, \boldsymbol{g}_2, \cdots, \boldsymbol{g}_k$，并考虑向量

$$\boldsymbol{u}=\lambda_1\boldsymbol{g}_1+\lambda_2\boldsymbol{g}_2+\cdots+\lambda_k\boldsymbol{g}_k$$

显然，$\boldsymbol{u}\in C$，且$\boldsymbol{u}$在坐标位置S上取零值。所以，$w(\boldsymbol{u})\leqslant n-(n-d+1)=d-1$。这个矛盾证明了定理的前一部分。

今设C的某个生成矩阵G中有一个向量$\boldsymbol{v}$，$w(\boldsymbol{v})=d$。令$\boldsymbol{v}$取零值的$n-d$个坐标为集合R，则G中具有列坐标R的$n-d$个列不可能包含信息组。否则，像前面的推理一样，会导致$\mathrm{rank}A<k$，从而产生矛盾。　　　　〈证毕〉

线性码的三个参数 n，k 和 d 之间有一定的制约关系。给定 n 和 k 后，一种关于 d 的上限是

定理2.5.6 （普洛特金（Plotkin）限）设 C 为二元（n，k，d）码，则

$$d \leqslant n \cdot 2^{k-1}/(2^k - 1) \tag{2-19}$$

为证明这一定理，我们需要下面的两个引理。

引理2.5.1 设二元（n，k）码 C 没有全零列，则在某固定列中为零的全体码字构成（n，$k-1$）码。

证明 不妨设该固定列是第一列，我们证明在第一列为零的 C 中全体码字的集合 C' 是 C 的 $k-1$ 维子空间。因为，若 $\boldsymbol{x}=(0x_2\cdots x_n)\in C'$，$\boldsymbol{y}=(0y_2\cdots y_n)\in C'$，则 $\boldsymbol{x}+\boldsymbol{y}=(0\ \cdots)\in C$，从而 $\boldsymbol{x}+\boldsymbol{y}\in C'$。所以，$C'$ 是 C 的子空间。此外，因 C 中没有全零列，故必有 $\boldsymbol{u}=(1\ \cdots)\in C$。于是，$C'$ 有两个不同的陪集 C' 和 $\boldsymbol{u}+C'$，且 $C=C'\cup(\boldsymbol{u}+C')$。因此，$C'$ 是 $k-1$ 维的。

〈证毕〉

引理2.5.2 设 C 是没有全零列的二元（n，k）码，则 C 中全体码字的重量之和为 $n\cdot 2^{k-1}$。

证明 设 A 为由 C 的全体码字组成的矩阵。由引理2.5.1，A 中任意列为零的行数为 2^{k-1}。因此，A 中每一个列都有 2^{k-1} 个1。但是，A 共有 n 列。所以，C 的总重量为 $n\cdot 2^{k-1}$。

〈证毕〉

定理2.5.6的证明 由引理2.5.2，没有全零列的二元（n，k，d）码 C 的总重量为 $n\cdot 2^{k-1}$。但是，C 中共有 2^k-1 个非零码字。因此，d 不能超过 C 的平均重量，即

$$d \leqslant n \cdot 2^{k-1}/(2^k - 1)$$

如果 C 中有全零列，则上式更加成立。 〈证毕〉

类似地，我们也可以证明关于 q 元（n，k，d）码的普洛特金限。这时，式（2-19）变为

$$d \leqslant n \cdot q^{k-1}(q-1)/(q^k - 1) \tag{2-20}$$

另一个（n，k）码的最小距离 d 能达到的上限是

定理2.5.7 （辛格里通（Singleton）限）设C是任意(n, k, d)码，则

$$d \leqslant n-k+1 \tag{2-21}$$

证明 设H为C的一致校验矩阵，则$\mathrm{rank}H=n-k$，因此，H中任意$n-k+1$列都线性相关。由定理2.5.4，则有

$$d \leqslant n-k+1$$

〈证毕〉

注意，式（2-21）对任意q元码都成立。特别，当$d=n-k+1$时，称q元(n, k, d)码C为**最大距离可分码**。此时，C的码字之间达到了最大可能的距离。由以上的讨论显然有，若H是最大距离可分码C的一致校验矩阵，则H中任意$n-k$列都线性无关。当给定n和k时，最大距离可分码是纠错能力最强的(n, k)码。

以上两个上限定理说明，对于某些参数n，k和d，(n, k, d)码是不存在的。最后，介绍一个下限定理，说明的确存在好的线性码。

定理2.5.8 （基尔伯特—瓦尔莎莫夫限（Gilbert-Varshamov））设下述不等式

$$\binom{n-1}{1}(q-1)+\binom{n-1}{2}(q-1)^2+\cdots+\binom{n-1}{d-2}(q-1)^{d-2} \leqslant q^s-1 \tag{2-22}$$

成立，则存在一个码长$=n$，维数$\geqslant n-s$且最小距离$\geqslant d$的q元码。

证明 我们构造一个$s \times n$矩阵H，使H中任意$d-1$列都线性无关，则由推论2.5.4.1可知，以H为一致校验矩阵的码C的最小重量$\geqslant d$。H的第1列可以为任意非零s重，第2列可以为除第1列的倍数以外的任意非零s重，第3列可以为除前两列的线性组合以外的任意s重，…等等。一般地，假定我们已经选定了i列，其中任意$d-1$列都线性无关，则从这i列中每次选

出 r 列（$r=1, 2, \cdots, d-2$），其所有不同的线性组合数为

$$\binom{i}{1}(q-1)+\binom{i}{2}(q-1)^2+\cdots+\binom{i}{d-2}(q-1)^{d-2}$$

(2-23)

如果式 (2-23)$<q^s-1$，则我们可以选取一个不同于这些线性组合的 s 重作为H的第 $i+1$ 列。我们可以一直这样作下去，直到当 $i=n$，使式 (2-23)$\geqslant q^s-1$ 时为止。此时，式 (2-22)成立，因此，H共有 n 列。由于$\mathrm{rank}H\leqslant s$，所以$C$的维数$\geqslant n-s$。 〈证毕〉

对于二元码，式 (2-22) 变为

$$\binom{n-1}{1}+\binom{n-1}{2}+\cdots+\binom{n-1}{d-2}<2^s-1 \qquad (2\text{-}24)$$

§2.6 汉明码和完备码

汉明码是50年代初期由汉明首先提出来的，是一种典型的性能良好的单纠错码类，其编码和译码都很容易实现。下面，我们探究一下汉明码产生的本源。

我们先从二元情形谈起。

设H为C的一致校验矩阵。我们知道，$r\in C$当且仅当 r 的伴随式 $s=rH'=0$。将接收向量 r 写成 $v+e$ 的形式,其中 $v\in C$，e 是错误向量，则有 $s=rH'=vH'+eH'=eH'$，即接收向量的伴随式等于错误格式的伴随式。因为

$$s'=(eH')'=He'=(h_1h_2\cdots h_n)\begin{pmatrix}e_1\\e_2\\\cdots\\e_n\end{pmatrix}$$

$$=e_1h_1+e_2h_2+\cdots+e_nh_n$$

其中 h_i 是H中的第 i 个列向量，所以我们得到下述重要结论：

接收向量的伴随式等于H矩阵中与信道错误相对应的各列之和。

特别，对于只出现单个错误的情形，例如第i位出错，即$e=(0\cdots0\ \underset{i}{1}\ 0\cdots0)$时，则有

$$s^t = He^t = h_i$$

由此可见，当H中有全零列时，则在该位置产生的错误将不会影响伴随式，因而无法检测出这种错误。例如，$h_1=0$，则无论$e=0$，还是$e=(1\ 0\cdots0)$，都有$s^t=He^t=0$。

如果H中有两列相同，则在两个位置之一所发生的单个错误与另一个所发生的单个错误具有相同的伴随式，于是这两种错误格式属于同一个陪集。因为只能选择其中之一作为陪集首，所以只能纠正其中之一的单个错误，另一个将不能正确译码。

因此，使二元线性码能够纠正所有单个错误格式的必要条件是（i）H中没有全零列；(ii) H中各列互不相同。

反之，若条件（i）和 (ii) 成立，则由推论2.5.4.1后面的讨论可知，$d\geqslant 3$，即上述条件也是充分的。综上所述，我们有

定理2.6.1 设H为二元(n, k, d)码C的一致校验矩阵，则$d\geqslant 3$当且仅当H中的各列均不相同且不为零。

现在我们考虑，对于最多有r个校验位的单纠错二元码C，其可能的码长n最长是多少呢？由于校验位的个数等于H矩阵的秩，因此上述问题归结为：在至多为r行的二元矩阵（即阵元取自$GF(2)$）中，所能出现的相异非零列的数目最大是多少，这一问题显然又等价于：用r位二进制数所能表示的正整数的最大数目是多少，答案是2^r-1，即用r位二进制数所能表示的全部正整数为

$$1,\ 2,\ 3,\ \cdots,\ 2^r-1$$

因此，H矩阵应由2^r-1个彼此相异的非零二元r维列向量组成，且$\operatorname{rank} H=r$。这是因为下述r个二元r维列向量

$$\begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix},\begin{pmatrix}0\\0\\\vdots\\1\\0\end{pmatrix},\cdots,\begin{pmatrix}0\\1\\\vdots\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\\vdots\\0\\0\end{pmatrix}$$

是H的一个极大线性无关列向量组。

经过以上准备，现在可以给出二元汉明码的定义了。

定义2.6.1 如果H矩阵由2^r-1（$r\geqslant 2$）个按任意顺序排列，且彼此相异的非零二元r维列向量组成，则以H为一致校验矩阵的线性分组码称为**二元汉明码**。

下面，我们讨论二元汉明码的三个重要参数n，k和d。显然，$n=2^r-1$，$k=n-r=2^r-1-r$。此外，由定理2.6.1，我们有$d\geqslant 3$。实际上，$d=3$。因为我们很容易找到一个重量为3的码字。例如

$$H=\begin{pmatrix}0&0&0&0&&1&1\\0&0&0&0&&1&1\\\vdots&\vdots&\vdots&\vdots&\cdots&\vdots&\vdots\\0&0&0&1&&1&1\\0&1&1&0&&1&1\\1&0&1&0&&0&1\end{pmatrix}$$

因为$\boldsymbol{h}_1+\boldsymbol{h}_2+\boldsymbol{h}_3=\boldsymbol{0}$，故（1 1 1 0 ⋯ 0）是一个重量为3的码字。

汉明码之所以重要，还在于在等价的意义上，它是唯一的单纠错完备码。我们只证明

定理2.6.2 二元汉明码是单纠错完备码。

证明方法1 陪集首至少有$n+1=2^r$个，即零向量和n个重量为1的向量。此外，每个陪集含有$2^k=2^{n-r}$个向量。因为，$(n+1)\cdot 2^{n-r}=2^r\cdot 2^{n-r}=2^n$，所以陪集首的最大重量为1，即汉明码是完备码。 〈证毕〉

方法2 因为汉明码是单纠错码，故以1为半径的码球互不相交。此外，每个码球中都含有$n+1=2^r$个向量，即位于码球

中心的向量及 n 个与它距离为 1 的向量。因为共有 $2^k=2^{n-r}$ 个码球，且 $(n+1)\cdot 2^{n-r}=2^n$，所以汉明码的覆盖半径等于 1。

（证毕）

例2.6.1 取 $r=2$，则 $n=2^r-1=3$，$k=n-r=1$。作

$$H=\begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\end{pmatrix}$$

则易得系统矩阵

$$G=(1\ 1\ 1)$$

因此，（3，1，3）二元汉明码只有两个码向量

$$(0\ 0\ 0),\ (1\ 1\ 1)$$

这是很明显的，因为除零向量之外，只有向量（1 1 1）的重量为 3。所以，不论 H 如何取法，G 总是（1 1 1）的形状。

这个码的标准阵列是

0 0 0　1 1 1

1 0 0　0 1 1

0 1 0　1 0 1

0 0 1　1 1 0

由此可见，半径为 1 的码球数＝码字数＝陪集中所含向量的个数 $=2^k=2^{n-r}=2^{3-2}=2$，且码球中的向量个数＝陪集个数 $=n+1=2^r=2^2=4$。

例2.6.2 取 $r=3$，则 $n=2^r-1=7$，$k=n-r=4$。按自然顺序排列 7 个二元 3 维列向量，所得到的矩阵形状为

$$H=\begin{pmatrix}0 & 0 & 0 & 1 & 1 & 1 & 1\\ 0 & 1 & 1 & 0 & 0 & 1 & 1\\ 1 & 0 & 1 & 0 & 1 & 0 & 1\end{pmatrix} \tag{2-25}$$

注意到，$\boldsymbol{h}_1+\boldsymbol{h}_2+\boldsymbol{h}_3=\boldsymbol{0}$，$\boldsymbol{h}_1+\boldsymbol{h}_6+\boldsymbol{h}_7=\boldsymbol{0}$，$\boldsymbol{h}_1+\boldsymbol{h}_4+\boldsymbol{h}_5=\boldsymbol{0}$，$\boldsymbol{h}_2+\boldsymbol{h}_4+\boldsymbol{h}_6=\boldsymbol{0}$，我们知道

$$\boldsymbol{a}=(1\ 1\ 1\ 0\ 0\ 0\ 0)$$

$$\boldsymbol{b}=(1\ 0\ 0\ 0\ 0\ 1\ 1)$$

$$\boldsymbol{c}=(1\ 0\ 0\ 1\ 1\ 0\ 0)$$

$$\boldsymbol{d}=(0\ 1\ 0\ 1\ 0\ 1\ 0)$$

是4个码向量，又因 $\boldsymbol{a}$，$\boldsymbol{b}$，$\boldsymbol{c}$，$\boldsymbol{d}$ 线性无关，于是以 $\boldsymbol{a}$，$\boldsymbol{b}$，$\boldsymbol{c}$ 和 $\boldsymbol{d}$ 为行的矩阵是一个与H相对应的生成矩阵

$$G=\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

为了更容易求出二元（7，4，3）汉明码的生成矩阵，我们作与系统矩阵G相对应的H矩阵如下：

$$H'=\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

即 $H'=[AI_3]$，其中 I_3 是 3×3 单位方阵，矩阵A中的任意列都至少包含2个1。因此，

$$G'=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

显然，由H和H'给出的两个码是彼此等价的。因为等价的码有相同的纠错能力和错误概率，所以它们没有本质的区别。

由于工程上的或其它原因，我们往往偏爱某种等价码。例如，第三种可能的H矩阵形为

$$H''=\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

注意，这时我们得到一个**循环码**，即码字循环移位后仍为码字。今后，我们将对循环码进行详尽的讨论。

二元汉明码的译码是极其简单的，尤其是采用形为式(2-25)

的H矩阵时，即$h_i = i$的r位二进制数形式。这时，为了对单个错误进行译码，译码器首先计算接收向量的伴随式s。如果$s=0$，则译码器判定没有发生错误。如果$s \neq 0$且$s=h_i$，则译码器判定第i位有错。如果$s \neq 0$且$s \neq h_j$，$j=1,2,\cdots,n$，则这种"不完全"译码方案失败。译码失败及译码错误仅当出现两个以上信道错误时才发生。

现在，我们对q元汉明码作一简短的讨论。粗看起来，将二元汉明码推广到q元（$q>2$）情形，只需作$r\times(q^r-1)$矩阵，使H矩阵由q^r-1个彼此不同的非零q元r维列向量组成即可。但这样作是行不通的，例如当$q=3$，$r=2$时，取

$$H=\begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

则有4对列向量$\begin{pmatrix}0\\1\end{pmatrix}$与$\begin{pmatrix}0\\2\end{pmatrix}$，$\begin{pmatrix}1\\0\end{pmatrix}$与$\begin{pmatrix}2\\0\end{pmatrix}$，$\begin{pmatrix}1\\1\end{pmatrix}$与$\begin{pmatrix}2\\2\end{pmatrix}$，$\begin{pmatrix}1\\2\end{pmatrix}$与$\begin{pmatrix}2\\1\end{pmatrix}$线性相关，因为其中一个是另一个的倍数。解决的办法是，每对只取其一，例如只取第一个非零元素为1的列向量。这时

$$H=\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$$

即为合乎要求的H矩阵。

因为非零q元r重共有q^r-1个，其中第一个非零元素为1者共有$(q^r-1)/(q-1)$个，所以H矩阵最多可有$(q^r-1)/(q-1)$列。

类似于二元情形，我们可以给出q元汉明码的定义。

定义2.6.2 如果H矩阵由$(q^r-1)/(q-1)$个$(q\geqslant 2, r\geqslant 2)$按任意顺序排列的非零$q$元$r$维列向量组成，其中任一列都不是其它列的倍数，则以$H$为一致校验矩阵的线性分组码称为$q$元汉明码。

显然，q元汉明码是$((q^r-1)/(q-1)\triangleq n,\ n-r,$

3）码。

平行于二元汉明码，我们有

定理2.6.3 q 元汉明码是单纠错完备码。

证明 证明完全类似于定理2.6.2的证明。注意到，此时共有 $q^k = q^{n-r}$ 个半径为1的码球，且每个码球中包含 $n(q-1)+1$ 个向量（位于码球中心的码字和 $n(q-1)$ 个与它距离为1的向量）。因为，$q^{n-r}(n(q-1)+1) = q^{n-r} \cdot q^r = q^n$。故定理得证。 〈证毕〉

例2.6.3 取 $q=3$，$r=2$，则 $n=4$，$k=n-r=2$。作

$$H=\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$$

则易得系统矩阵

$$G=\begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & -2 \end{pmatrix}=\begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

可见，这个三元（4，2，3）汉明码的 $3^2 = 9$ 个码字是

$$\begin{array}{lll} (0\ 0\ 0\ 0), & (0\ 1\ 2\ 1), & (0\ 2\ 1\ 2) \\ (1\ 0\ 2\ 2), & (1\ 1\ 1\ 0), & (1\ 2\ 0\ 1) \\ (2\ 0\ 1\ 1), & (2\ 1\ 0\ 2), & (2\ 2\ 2\ 0) \end{array} \qquad (2\text{-}26)$$

此外，在这个码的标准阵列中，下述9个向量

$$\begin{array}{lll} (0\ 0\ 0\ 0), & (1\ 0\ 0\ 0), & (2\ 0\ 0\ 0) \\ (0\ 1\ 0\ 0), & (0\ 2\ 0\ 0), & (0\ 0\ 1\ 0) \\ (0\ 0\ 2\ 0), & (0\ 0\ 0\ 1), & (0\ 0\ 0\ 2) \end{array}$$

为陪集首。

回过头来再看例2.2.2，显然以式（2-12）为生成矩阵 G 的三元码是（4，2，3）汉明码。这两个码是等价的，因为我们可以通过矩阵行的初等变换和列的置换将其中一个码的生成矩阵变成另一个的生成矩阵。事实上

$$\begin{pmatrix}1&0&2&2\\0&1&2&1\end{pmatrix}\xrightarrow{(2)+(1)}\begin{pmatrix}1&1&1&0\\0&1&2&1\end{pmatrix}$$

$$\xrightarrow{(1)+(2)}\begin{pmatrix}1&1&1&0\\1&2&0&1\end{pmatrix}\Longrightarrow\begin{pmatrix}1&0&1&1\\0&1&2&1\end{pmatrix}$$

最后一个矩阵变换是列的置换，我们将左边矩阵的第 1， 2， 3， 4 列变成右边矩阵的第 4， 3， 1， 2 列。

因此，对式（2-26）中的 9 个码字作列的置换

$$\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}$$

就得到例 2.2.2 中的 9 个码字。下边我们将这两个三元（4，2，3）汉明码排在一起，将例 2.2.2 中的码字放在右边。

0 0 0 0	0 0 0 0
1 0 2 2	2 2 0 1
2 0 1 1	1 1 0 2
0 1 2 1	2 1 1 0
1 1 1 0	1 0 1 1
2 1 0 2	0 2 1 2
0 2 1 2	1 2 2 0
1 2 0 1	0 1 2 1
2 2 2 0	2 0 2 2

既然 q 元汉明码是完备码，那么，还有其它的 q 元码是完备码吗？如有，应沿什么方向去寻找它们呢？因为此时覆盖半径 r 等于球包半径 t，故 n、k 和 d 之间必定存在着某种制约关系。所以，不应该漫无目的地去寻求任意码长 n 的完备码，而应首先寻找这种制约关系。其办法是，计算以 t 为半径的码球个数，乘以码球中所含向量的个数，并令其乘积等于整个向量空间 V_n 中的向量数。如此得

定理2.6.4 q 元（n，k，d）码是完备码的必要条件是

$$\left(\binom{n}{0}+(q-1)\binom{n}{1}+\cdots+(q-1)^t\binom{n}{t}\right)q^k=q^n \quad (2\text{-}27)$$

特别，当 $q=2$ 时，式（2-27）变为

$$\left(\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}\right)2^k=2^n \tag{2-28}$$

称 $\boldsymbol{h}\triangleq(1\ 1\cdots 1)$ 为全1向量。当 n 为奇数时，由全1向量生成的二元（n，1，n）码 $\langle\boldsymbol{h}\rangle$ 显然是完备码。此外，整个空间 V_n 当然也是完备码。称上述两类完备码为**平凡完备码**。我们所关心的是除此之外的**非平凡完备码**。

现在考虑二元完备码存在的必要条件。当 $t=1$ 时，我们有 $(1+n)2^k=2^n$，因此 $n=2^{n-k}-1$。如令 $r=n-k$，则有 $n=2^r-1$，$k=n-r=2^r-1-r$，以及 $d=3$。这正是二元汉明码所具有的参数。当 $t=2$ 时，必要条件变为 $\left(1+n+\binom{n}{2}\right)2^k=2^n$，或 $1+n+\binom{n}{2}=2^{n-k}$。因此，$1+n+\binom{n}{2}$ 必为2的某次幂。满足这个条件的最小的 n 值是5，与之对应的是二元（5，1，5）平凡完备码。第2个 n 值是90，可以证明 $n=90$ 的完备码不存在（参看§7.5）。当 $t=3$ 时，以3为半径的码球包含 $1+n+\binom{n}{2}+\binom{n}{3}$ 个向量，当 $n=23$ 时使之变成2的11次幂。这就得到著名的二元（23，12，7）完备码，称之为戈莱（Golay）码。

类似地，在三元码情形中，为使双纠错完备码存在，必须令 $1+2n+4\binom{n}{2}$ 为3的某次幂。注意到当 $n=11$ 时，$1+2\cdot 11+2\cdot 11\cdot 10=243=3^5$。这就得到三元（11，6，5）完备码——另一种著名的戈莱码。

对于任意 q 元（n，k，d）码 C，或者 C 是完备码，或者 C 的以 t 为半径的码球外边还有 V_n 中的向量，二者必居其一。如

此就证明了下面的定理。

定理2.6.5 （汉明球包限）设C为q元（n，k，d）码，则有

$$\left(\binom{n}{0}+(q-1)\binom{n}{1}+\cdots+(q-1)^t\binom{n}{t}\right)q^k\leqslant q^n \tag{2-29}$$

注意，当给定n和k后，汉明球包限限定了t，因而给出了d的上限。例如，当$q=2$，$n=7$，$k=4$时，我们有

$$\binom{7}{1}+\binom{7}{2}+\cdots\leqslant 2^3-1=7$$

可见，$t=1$。因而，二元（7，4）码最多只能纠一个错。

鉴于完备码是给定n和k后，纠错能力最强的码，以及其它多种原因，人们对完备码进行了大量的深入研究。美中不足的是，研究结果表明，完备码的种类是很少的。我们不加证明地给出下述定理，这是关于完备码研究的一个完整的总结。

定理2.6.6 唯一的非平凡多纠错完备码等价于二元（23，12，7）戈莱码或三元（11，6，5）戈莱码。唯一的非平凡单纠错完备码与汉明码有相同的参数。

尽管完备码屈指可数，但令人欣慰的是，拟完备码却是大量存在的。

下面，我们讨论汉明码的检错问题。为此，我们要作一些准备。

定义2.6.3 设C为q元（n，k，d）码，称C^*为C的**扩展码**，如果

$$C^*\triangleq\left\{(c_1,\ \cdots,\ c_n,\ c_{n+1})\,|\,(c_1,\ \cdots,\ c_n)\in C,\ \sum_{i=1}^{n+1}c_i=0\right\}$$

由定义可见，对C的每一个码字都增加一个全一致校验位，就得到扩展码C^*。因此，在二元情形中，当d为奇数时，C^*是（$n+1$，k，$d+1$）码，因为C^*中只包含偶重量向量。

设C的生成矩阵和一致校验矩阵分别为G和H。于是，C^*的生成矩阵G^*由G增加一列而得到，使得G^*的各列之和等于零向量。此外，H^*具有如下形状：

$$H^*=\begin{pmatrix} 1 & 1 \cdots 1 \\ & H \quad \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \end{pmatrix}$$

这是因为H^*由H增加一行和一列得到，且G^*与H^*之间必须满足关系

$$GH'=O, \quad HG'=O$$

即G^*中任意行与H^*中任意行一定正交。

扩展码的逆过程是删除码的一列，因而有

定义2.6.4 设C为q元（n，k，d）码，称$\hat{C}$为C的**删除码**，如果C的生成矩阵G删除一列后成为$\hat{C}$的生成矩阵$\hat{G}$。

注意，给定C后，删除不同的列可能得到不等价的码。删除码的码长为$n-1$，维数为k或$k-1$，最小距离通常是$d-1$，但也有可能为d。

通常，我们采用扩展与删除码的方法获得各种合乎需要的码类。下述二元扩展汉明码就是其中一例。

例2.6.4 设$r=4$，则$n=2^4-1=15$，$k=n-r=11$。二元（15，11，3）汉明码C的一致校验矩阵为

$$H=\begin{pmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix}$$

因此，二元（16，11，4）扩展汉明码C^*的一致校验矩阵

$$H^*=\begin{pmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0 \end{pmatrix}$$

接收向量 r 的伴随式 $s^t=H^*r^t=H^*e^t$ 是 H^* 矩阵中与信道出现的错误相对应的各列之和，我们有如下的译码方法。如果没有错误发生，则 $\mathbf{s}=\mathbf{0}$。如果发生一个错误，例如信道第 i 位出错，则有

$$\mathbf{s}^t=\begin{pmatrix}1\\w\\x\\y\\z\end{pmatrix}$$

其中 $(w\ x\ y\ z)$ 是 i 的二进制数形式。如果发生两个错误，则

$$\mathbf{s}^t=\begin{pmatrix}0\\w\\x\\y\\z\end{pmatrix}$$

此时译码器断定有两个（或更多）错误发生，但无法进行纠错。

显然，这个特例具有一般性。因此，扩展汉明码可以纠正重量$\leqslant 1$的所有错误的错误格式，并能发现重量为 2 的错误格式。为此，有时称为“纠 1 检 2”码。

最后，顺便指出，汉明码是信息率很高的码。事实上，二元 $(n, n-r)$ 码的信息率 $R=k/n=(n-r)/n=1-r/n$。所以，当 r 给定以后，n 越大 R 就越大。二元汉明码的码长 $n=2^r-1$，使 R 达到极大值 $1-r/(2^r-1)$。

扩展汉明码的信息率为

$$R=1-(r+1)/n=1-(r+1)/2^r$$

当 n 很大时，汉明码和扩展汉明码的信息率都接近于 1。

以下是关于汉明码的小结。

汉明码小结

主要参数

码长 $n=(q^r-1)/(q-1)$　$(q\geqslant 2,\ r\geqslant 2)$

维数 $k = n - r$

校验位数 $= r$

最小距离 $d = 3$

重要性质

（1）在等价的意义上，汉明码是唯一的单纠错完备码；

（2）一致校验矩阵H是 $r \times n$ 矩阵，它的列是非零 q 元 r 重，其中任一列都不是其它列的倍数。

§2.7 自正交码与自对偶码

回忆我们在§2.3中给出的关于对偶码的定义，称$C^{\perp}$是C的对偶码，如果

$$C^{\perp} = \{u \in V_n | u \perp v, \text{对一切 } v \in C\}$$

对偶码的概念为研究码提供了一个有力的工具。今后我们将看到，从对偶码$C^{\perp}$可以揭示有关原码C的许多特性。因此，我们常常将C和$C^{\perp}$结合在一起进行研究。

本节将要讨论两种C与$C^{\perp}$联系得十分紧密的码，自正交码与自对偶码。它们都具有一些特别的结构。

定义2.7.1 称(n, k)码C为**自正交码**，如果$C \subseteq C^{\perp}$。

由定义可见，自正交码有两个特点：（i）C中任意码字都和它自身正交。因此，在二元自正交码中，所有码字的重量都是偶数。同理，在三元自正交码中，所有码字的重量都是3的倍数(注意在$GF(3)$中，$2 \cdot 2 = 1$，$1 + 1 + 1 = 0$)。(ii) C中任意两个码字都互相正交。

定义2.7.2 设$\boldsymbol{x} = (x_1, \cdots, x_n)$和$\boldsymbol{y} = (y_1, \cdots, y_n)$为任意向量，则$\boldsymbol{x}$和$\boldsymbol{y}$的乘积定义为

$$\boldsymbol{x} * \boldsymbol{y} \triangleq (x_1 y_1, \cdots, x_n y_n)$$

因此，对于二元向量x和y，若$u = (u_1, \cdots, u_n) = \boldsymbol{x} * \boldsymbol{y}$，则$u_i = 1$当且仅当$x_i = y_i = 1$。于是，$w(\boldsymbol{x} * \boldsymbol{y})$表示$\boldsymbol{x}$和$\boldsymbol{y}$中对应坐标皆为1的坐标个数。不难证明，下述十分有用的公式成立：

$$w(\boldsymbol{x}+\boldsymbol{y})=w(\boldsymbol{x})+w(\boldsymbol{y})-2w(\boldsymbol{x}*\boldsymbol{y}) \qquad (2\text{-}30)$$

值得注意的是，式（2-30）仅适用于二元向量。

下面的定理是二元和三元自正交码的判定准则。

定理2.7.1 设G为二元（n，k）码C的生成矩阵。如果G的行重量皆为偶数且各行彼此正交，则C是自正交码，反之亦真。

设G'为三元（n，k）码C'的生成矩阵。如果G'的行重量为3的倍数且各行互相正交，则C'是自正交码，反之亦真。

证明 我们只证明二元码的情形。对于C'的证明是完全类似的。

首先，因为G的任意行的重量都是偶数，所以G中的行与它自身正交。其次，根据假设，G中任意两行都彼此正交。设$\boldsymbol{x}$和$\boldsymbol{y}$为C中任意两个向量(相同或相异)，则$\boldsymbol{x}$和$\boldsymbol{y}$都是G中诸行的线性组合。由于内积的线性性质，$\boldsymbol{x}\cdot\boldsymbol{y}=(\alpha_1\boldsymbol{g}_1+\cdots+\alpha_k\boldsymbol{g}_k)\cdot(\beta_1\boldsymbol{g}_1+\cdots+\beta_k\boldsymbol{g}_k)=\alpha_1\beta_1(\boldsymbol{g}_1\cdot\boldsymbol{g}_1)+\cdots+\alpha_k\beta_1(\boldsymbol{g}_k\cdot\boldsymbol{g}_1)+\cdots=0$，其中$\boldsymbol{g}_1$，…，$\boldsymbol{g}_k$是$G$的行向量，$\alpha_i$，$\beta_j\in GF(2)$。因此，$C$是自正交码。

反之，若C为自正交码，则因G中诸行都是C中的码字，故G的行重量皆为偶数且各行互相正交。〈证毕〉

对于二元（n，k）码，进一步还有

定理2.7.2 设G为二元（n，k）码C的生成矩阵。如果G的行重量为4的倍数且各行互相正交，则C为自正交码，且C中所有码字的重量都是4的倍数。

证明 由定理2.7.1，C是自正交码。剩下来只需证明C中所有码字的重量都是4的倍数。由假设，G中任意行的重量都是4的倍数。设$\boldsymbol{g}_1$和$\boldsymbol{g}_2$是G中的行，则由式（2-30），$w(\boldsymbol{g}_1+\boldsymbol{g}_2)=w(\boldsymbol{g}_1)+w(\boldsymbol{g}_2)-2w(\boldsymbol{g}_1*\boldsymbol{g}_2)$。因为$\boldsymbol{g}_1\perp\boldsymbol{g}_2$，故$w(\boldsymbol{g}_1*\boldsymbol{g}_2)$为偶数，所以$w(\boldsymbol{g}_1+\boldsymbol{g}_2)$是4的倍数。用数学归纳法易证，$G$中诸行的任意线性组合都是4的倍数。〈证毕〉

例2.7.1 考虑例2.6.2中以G'为生成矩阵的二元（7，4，

3）汉明码C，如果增加一个一致校验位，就得到二元（8，4，4）扩展汉明码C^*，其生成矩阵为

$$G^*=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

由定理2.7.2，C^*是自正交码，且C^*中所有码字的重量都是4的倍数。C^*中有1个重量为8的向量，14个重量为4的向量和1个零向量。

在刚才的例子中，我们统计码C^*中具有不同重量的码字的个数，这是一件很有意义的工作。

定义2.7.3 称集合$\{A_i\}$为码C的**重量分布**，如果C中重量为i的码字有A_i个。

注意，任意线性分组码都含有零向量。因此，我们总有$A_0=1$。在同时讨论C及其对偶码$C^\perp$的重量分布时，$C^\perp$的重量分布常常用集合$\{B_i\}$表示。

如何计算码C的重量分布呢？当然，最直接的办法是列出C中所有的码字，然后计算C的重量分布。但是当n很大时，这种方法是不现实的。因此设计行之有效的计算码的重量分布的方法，是编码理论的一个重要任务。今后我们将看到，通过C与$C^\perp$的重量分布之间的联系，是解决这个问题的一种途径。

例2.7.2 将例2.7.1中的G^*去掉最后一列，就得到例2.6.2中的G'。我们求以G'为生成矩阵的二元（7，4，3）汉明码C的重量分布。

注意到$A_0=1$，$d=3$，且G'中各行之和为全1向量$\mathbf{h}$，即$A_7=1$。因此如果$v\in C$，则$v+h\in C$。于是，对于C中所有其它的向量，其重量必为3或4，且重量等于3和4的向量一定成对出现。由此可见，$A_0=A_7=1$，$A_3=A_4=7$。

至于以G^*为生成矩阵的扩展二元（8，4，4）汉明码，由

上述结果易得，C^*的重量分布是 $A_0^* = A_8^* = 1$， $A_4^* = 14$

再看一个求重量分布的例子。

例2.7.3 设二元（7， 3）码C的生成矩阵为

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

由定理2.7.2，C是自正交码，且$A_i = 4t$。但$n = 7$，可见$A^0 = 1$，$A_4 = 7$。这个例子告诉我们，自正交码往往对计算重量分布提供方便。

因此，$C^\perp$是以C的一致校验矩阵

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

为生成矩阵的（7， 4）码。因为G中的任意行都是H中诸行的线性组合，所以我们验证了$C \subseteq C^\perp$的正确性。不难看出，$C^\perp = C + \langle \boldsymbol{h} \rangle$，即在$G$中增加一个全1行后，就得到$C^\perp$。

通过类似于例2.7.2中的推理，由$\{A_i\}$极易求得$C^\perp$的重量分布：$B_0 = B_7 = 1$，$B_3 = B_4 = 7$。

上述例题具有一般性，这就是

定理2.7.3 设n为奇数，C为二元$(n, (n-1)/2)$自正交码，则$C^\perp$是$(n, (n+1)/2)$码，且$C^\perp = C + \langle \boldsymbol{h} \rangle$。

证明 因为C是$(n-1)/2$维的，故$C^\perp$是$n - (n-1)/2 = (n+1)/2$维的，即$C^\perp$是$(n, (n+1)/2)$码，且由假设，$C \subseteq C^\perp$。由于C中所有码字的重量都是偶数，故$\boldsymbol{h} \in C^\perp$。但是，$n$为奇数，故$\boldsymbol{h} \overline{\in} C$。因此，$C^\perp = C + \langle \boldsymbol{h} \rangle$。 〈证毕〉

定义 2.7.4 称(n, k)码C为自对偶码，如果$C = C^\perp$。

显然，自对偶码存在的必要条件是n为偶数，且$k = n/2$，即C必须是$(n, n/2)$码。注意，这一条件并不充分。但当

C是自对偶码时，上述条件就变成充分的了。因此，C是自对偶码当且仅当C是（n，$n/2$）自正交码，其中n为偶数。

由此可知，例2.7.1中的二元（8，4，4）扩展汉明码C^*是自对偶码。而例2.6.3中的三元（4，2，3）汉明码C，则是三元自对偶码的例子。因此

$$G=\begin{pmatrix}1 & 0 & -1 & -1\\ 0 & 1 & -1 & -2\end{pmatrix}$$

和

$$H=\begin{pmatrix}1 & 1 & 1 & 0\\ 1 & 2 & 0 & 1\end{pmatrix}$$

都是C的生成矩阵。一般地，我们有

定理2.7.4 设C是（n，$n/2$）自对偶码，且以$[IA]$为生成矩阵，则$[-A'I]$也是C的生成矩阵。

证明 设$G=[IA]$为C的生成矩阵，则$H=[-A'I]$为C的一致校验矩阵，故为$C^{\perp}$的生成矩阵。但$C=C^{\perp}$，因此$H=[-A'I]$也是C的生成矩阵。 〈证毕〉

上述定理再一次显示出系统码的优越性。

当n为偶数时，二元（n，$n/2$）自对偶码总是存在的，因为只要G形如

$$G=\begin{pmatrix}1 & 1 & 0 & 0\cdots 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 1\cdots 0 & 0 & 0 & 0\\ & \vdots & & \cdots & \vdots & & \\ 0 & 0 & 0 & 0\cdots 1 & 1 & 0 & 0\\ 0 & 0 & 0 & 0\cdots 0 & 0 & 1 & 1\end{pmatrix}$$

则以G为生成矩阵的（n，$n/2$）码是自正交码，因而是自对偶码。

对于三元自对偶码，情况就不同了。我们不加证明地给出以下结果。

三元（n，$n/2$）自对偶码存在当且仅当n是 4 的倍数。

定义2.7.5 称二元（n，$n/2$）自对偶码C为双偶码，如果$A_i=0$，对一切$i\neq 4t$。

例 2.7.2 中的二元（8，4，4）扩展汉明码C^*是双偶码，因为它的重量分布为$A_0^*=A_8^*=1$，$A_4^*=14$。而例 2.7.3 中的二元（7，3）码C，尽管它的重量分布是$A_0=1$，$A_4=7$，但它不是自对偶码（C只是自正交码），因而不是双偶码。

一般地，我们有以下结果：**双偶（n，$n/2$）码存在当且仅当n为 8 的倍数。**其证明从略。

最后，我们以两个最重要的自对偶码，二元和三元戈莱码结束本节和本章。

二元（24，12）戈莱码C由生成矩阵$G=[I\ A]$给出，其中

$$A=\begin{pmatrix}
 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & 1 & 1 & & 1 & 1 & 1 & & & & 1 & \\
1 & 1 & & 1 & 1 & 1 & & & & 1 & & 1\\
1 & & 1 & 1 & 1 & & & & 1 & & 1 & 1\\
1 & 1 & 1 & 1 & & & & 1 & & 1 & 1 & \\
1 & 1 & 1 & & & & 1 & & 1 & 1 & & 1\\
1 & 1 & & & & 1 & & 1 & 1 & & 1 & 1\\
1 & & & & 1 & & 1 & 1 & & 1 & 1 & 1\\
1 & & & 1 & & 1 & 1 & & 1 & 1 & 1 & \\
1 & & 1 & & 1 & 1 & & 1 & 1 & 1 & & \\
1 & 1 & & 1 & 1 & & 1 & 1 & 1 & & & \\
1 & & 1 & 1 & & 1 & 1 & 1 & & & & 1
\end{pmatrix}$$

A是 12×12 方阵，A中的空白表示零，而I是 12×12 单位方阵。由定理 2.7.2，C为双偶码，因而$A_i=4t$。

下面我们试求C的最小重量d。如果采用最原始的方法，列出2^{12}个码字，然后一一计算其重量，则显然太烦琐了。注意到

C是双偶码，故$d=4$或8。我们证明，$d=8$。先看G中任意两行之和的重量，这时分成两种情况：（i）当第一行是其中一行时，由于A中其余各行都有1个1在第一位，有6个1在其余11位，故立即可得和的重量为8，（ii）当第一行不在其内时，对于A中任意两行$\boldsymbol{a}$和$\boldsymbol{a}'$都有$w(\boldsymbol{a}*\boldsymbol{a}')=4$，因此和的重量也是8。其次考虑$G$中任意三行之和，它的重量也不能等于4。假定不然，则有$\boldsymbol{x}=(\boldsymbol{y},\boldsymbol{z})\in C$，其中$\boldsymbol{y}$和$\boldsymbol{z}$都有12个坐标，且$w(\boldsymbol{y})=3$，$w(\boldsymbol{z})=1$。但是$A^t=A$，故由定理2.7.4，$G'=[-A^tI]=[AI]$也是$C$的生成矩阵，因此$\boldsymbol{x}$是$G'$中的一行。显然$G'$中并没有重量等于4的行，故而产生矛盾。最后考虑$G$中任意4行之和的重量，不难看出它也不是4。因为$A$中任意三行之和的重量为5或9，而$A$中任意一行之重量为7或11，无论如何$A$中任意4行之和皆不可能为零向量。因为$G$中5行以上和的重量$\geqslant 8$，故$d=8$。

将G中所有的行相加，我们有$\boldsymbol{h}\in C$。因此，C中的码字只可能有下述重量

$$0,\ 8,\ 12,\ 16,\ 24$$

且$A_0=A_{24}=1$，$A_8=A_{16}$。关于二元戈莱码的重量分布问题，我们将留待后面的章节中解决。

三元（12，6）戈莱码C的生成矩阵为$G=[IA]$，其中I为6×6单位方阵，A为6×6方阵。

$$A=\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

由定理2.7.1，C是自正交码，因而是自对偶码。所以$A_i=3t$。

类似于二元戈莱码，我们可以证明三元戈莱码的最小重量 d 不是3而是6。首先，G 中任意两行之和的重量不等于3。否则存在 $\boldsymbol{x}=(\boldsymbol{y},\ \boldsymbol{z})\in C$，且 $w(\boldsymbol{y})=2$，$w(\boldsymbol{z})=1$。但是 $G'=[-A'I]=[-AI]$ 也是 C 的生成矩阵，故 x 是 G' 中的一行。然而 G' 中并没有重量等于3的行。其次 G 中任意三行之和的重量也不可能为3。因为 A 中任意两行之和的重量为4，故 A 中任意三行之和不可能等于零向量。因此 $d=6$。

无论从理论价值还是从实践角度来看，戈莱码都属于最重要的码类。今后我们还会遇到它们。

第三章　编码理论中的某些代数概念

§3.1　欧几里德算法及其应用

进一步研究编码理论，涉及到许多数学上的，特别是近世代数方面的概念。为使本书尽量自成体系，这一章就编码理论中经常用到的数学背景知识，主要是代数等方面的内容，作一扼要的介绍。

我们先从数论中的一些概念谈起。

设 a 为任一实数，用 $[a]$ 表示不超过 a 的最大整数，例如，

$$[5]=5,\ [\sqrt{3}]=1,\ [-3.5]=-4$$

称 $[a]$ 为**实数 a 的整数部分**。显然有

$$[a]\leqslant a<[a]+1 \tag{3-1}$$

定理3.1.1　（欧几里德除法）设 b 是正整数，则任意整数 a 可以唯一地写成下列形式

$$a=bq+r\qquad 0\leqslant r<b \tag{3-2}$$

证明　取 $q=[a/b]$，则由式（3-1），

$$\left[\frac{a}{b}\right]\leqslant\frac{a}{b}<\left[\frac{a}{b}\right]+1$$

或

$$0\leqslant a-b\left[\frac{a}{b}\right]<b$$

令 $r=a-b\left[\frac{a}{b}\right]$，则 $0\leqslant r<b$，并且

$$a=b\left[\frac{a}{b}\right]+r=bq+r$$

现在证明唯一性。假如另有

$$a=bq_1+r_1\qquad 0\leqslant r_1<b$$

则由式（3-2），

$$0=b(q-q_1)+(r-r_1)$$

可见，$(r-r_1)$ 是 b 的倍数。但是，$|r-r_1|<b$，因此 $r=r_1$，从而 $q=q_1$。 〈证毕〉

多项式的除法性质与整数的除法性质是完全类似的，平行于定理3.1.1，我们有：

定理3.1.2 （欧几里德除法）设 $b(x)$ 为非零多项式，则任意多项式 $a(x)$ 可以唯一地写成

$$a(x)=b(x)q(x)+r(x) \tag{3-3}$$

其中 $\deg r(x)<\deg b(x)$ 或 $r(x)=0$

$\deg f(x)$ 表示多项式 $f(x)$ 中系数不等于零的最高次项的次数。特别，对于**零多项式** $f(x)=0$，规定 $\deg 0=-\infty$。

定义3.1.1 设 a_1，a_2，…，a_n 为不全为零的整数，我们称能同时整除它们的正整数为 a_1，a_2，…，a_n 的**公约数**，称公约数中最大者为**最大公约数**，并记为 $(a_1, a_2, \cdots, a_n)$。如果 $(a_1, a_2, \cdots, a_n)=1$，则称 a_1，a_2，…，a_n 是**互素**的。

对于多项式，相应地定义同时除尽多项式 $a_1(x)$，$a_2(x)$，…，$a_n(x)$（它们不全为零多项式）**的多项式为公因式**，其中公因式中次数最高者称为**最高公因式**，记为 $(a_1(x), a_2(x), \cdots, a_n(x))$。

与整数情形有所不同，设 $g(x)$ 为某个最高公因式，则 $cg(x)$ 亦然，其中 $c\neq 0$。因此，为确定起见，我们约定最高公因式为**首一多项式**，即首项系数（多项式的最高次项的系数）为1的多项式。

如果 $(a_1(x), a_2(x), \cdots, a_n(x))=1$，则称多项式 $a_1(x)$，$a_2(x)$，…，$a_n(x)$ 是**互素**的。

求整数的最大公约数和多项式的最高公因式，要分别利用关于整数的和关于多项式的欧几里德算法，或称辗转相除法。

定理3.1.3 （欧几里德算法）给定多项式 $r_{-1}(x)$ 和 $r_0(x)$ 其中 $\deg r_0\leqslant\deg r_{-1}$。反复进行欧几里德除法，得到下列方程式：

$$r_{-1}(x)=q_1(x)r_0(x)+r_1(x),\quad \deg r_1<\deg r_0$$

$$r_0(x)=q_2(x)r_1(x)+r_2(x),\quad \deg r_2<\deg r_1$$

$$\cdots\cdots$$

$$r_{l-2}(x)=q_l(x)r_{l-1}(x)+r_l(x),\quad \deg r_l<\deg r_{l-1}$$

$$r_{l-1}(x)=q_{l+1}(x)r_l(x)$$

于是，$r_l(x)=(r_{-1}(x),\ r_0(x))$

证明 因为$r_l(x)$整除$r_{l-1}(x)$，故整除$r_{l-2}(x)$，…，因此整除$r_0(x)$和$r_{-1}(x)$，即$r_l(x)$是$r_0(x)$和$r_{-1}(x)$的公因式。今设$h(x)$整除$r_0(x)$和$r_{-1}(x)$，则$h(x)$整除$r_1(x)$，$r_2(x)$，…，$r_l(x)$。因此，$r_l(x)=(r_0(x),\ r_{-1}(x))$。 〈证毕〉

进一步，我们还有

定理3.1.4 给定多项式$r_{-1}(x)$和$r_0(x)$，其中$\deg r_0\leqslant\deg r_{-1}$，且$(r_{-1}(x),\ r_0(x))=h(x)$。于是，存在多项式$A(x)$和$B(x)$，使

$$A(x)r_{-1}(x)+B(x)r_0(x)=h(x) \tag{3-4}$$

其中 $\deg A<\deg r_{-1}$，$\deg B<\deg r_{-1}$

证明 我们定义多项式$A_i(x)$和$B_i(x)$如下：

$$A_{-1}(x)=0,\quad A_0(x)=1$$

$$B_{-1}(x)=1,\quad B_0(x)=0$$

当$i\geqslant 1$时，

$$\left.\begin{aligned}A_i(x)&=q_i(x)A_{i-1}(x)+A_{i-2}(x)\\B_i(x)&=q_i(x)B_{i-1}(x)+B_{i-2}(x)\end{aligned}\right\} \tag{3-5}$$

将式(3-5)写成矩阵形式，并利用递推关系，我们有

$$\begin{aligned}\begin{bmatrix}A_i(x) & A_{i-1}(x)\\ B_i(x) & B_{i-1}(x)\end{bmatrix}&=\begin{bmatrix}A_{i-1}(x) & A_{i-2}(x)\\ B_{i-1}(x) & B_{i-2}(x)\end{bmatrix}\begin{bmatrix}q_i(x) & 1\\ 1 & 0\end{bmatrix}\\&=\cdots\\&=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}q_1(x) & 1\\ 1 & 0\end{bmatrix}\cdots\begin{bmatrix}q_i(x) & 1\\ 1 & 0\end{bmatrix}\end{aligned} \tag{3-6}$$

此外，由欧几里德算法，

$$\begin{bmatrix} r_{i-2}(x) \\ r_{i-1}(x) \end{bmatrix}=\begin{bmatrix} q_i(x) & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} r_{i-1}(x) \\ r_i(x) \end{bmatrix}$$

$$\begin{bmatrix} r_{i-3}(x) \\ r_{i-2}(x) \end{bmatrix}=\begin{bmatrix} q_{i-1}(x) & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} r_{i-2}(x) \\ r_{i-1}(x) \end{bmatrix}$$

$$=\begin{bmatrix} q_{i-1}(x) & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} q_i(x) & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} r_{i-1}(x) \\ r_i(x) \end{bmatrix}$$

$$\cdots$$

$$\begin{bmatrix} r_{-1}(x) \\ r_0(x) \end{bmatrix}=\begin{bmatrix} q_1(x) & 1 \\ 1 & 0 \end{bmatrix}\cdots\begin{bmatrix} q_{i-1}(x) & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} q_i(x) & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} r_{i-1}(x) \\ r_i(x) \end{bmatrix}$$

$$=\begin{bmatrix} A_i(x) & A_{i-1}(x) \\ B_i(x) & B_{i-1}(x) \end{bmatrix}\begin{bmatrix} r_{i-1}(x) \\ r_i(x) \end{bmatrix} \tag{3-7}$$

显然，式（3-6）右端的行列式$=(-1)^i$。因此，由式（3-6)和式（3-7）得

$$\begin{bmatrix} r_{i-1}(x) \\ r_i(x) \end{bmatrix}=(-1)^i\begin{bmatrix} B_{i-1}(x) & -A_{i-1}(x) \\ -B_i(x) & A_i(x) \end{bmatrix}\begin{bmatrix} r_{-1}(x) \\ r_0(x) \end{bmatrix}$$

特别地，

$$r_i(x)=(-1)^i[-B_i(x)r_{-1}(x)+A_i(x)r_0(x)] \tag{3-8}$$

此即式（3-4)。此外，我们有

$$\deg A_i=\sum_{k=1}^{i}\deg q_k$$

$$\deg r_{i-1}=\deg r_{-1}-\sum_{k=1}^{i}\deg q_k$$

因此，

$$\deg A_i=\deg r_{-1}-\deg r_{i-1}<\deg r_{-1}$$

由于 $\deg r_i<\deg r_0\leqslant\deg r_{-1}$，故根据式（3-8)，

$$\deg B_i\leqslant\deg A_i<\deg r_{-1}$$

〈证毕〉

不言而喻，对于整数我们有相应的结果。

定理3.1.5 给定整数 a，b，必存在整数 A，B，使

$$aA+bB=(a,\ b)$$

例3.1.1 求二元多项式（即系数取自 $GF(2)$ 的多项式）$r_{-1}(x)=x^5+x^3+x+1$ 和 $r_0(x)=x^3+x^2+x+1$ 的最高公因式。

由欧几里德算法

$$x^5+x^3+x+1=(x^2+x+1)(x^3+x^2+x+1)+(x^2+x)$$

$$x^3+x^2+x+1=x(x^2+x)+(x+1)$$

$$x^2+x=x(x+1)$$

因此，$r_2(x)=x+1=(x^5+x^3+x+1,\ x^3+x^2+x+1)$

此外，我们有

$$A_{-1}(x)=0,\quad A_0(x)=1$$

$$A_1(x)=q_1(x)=x^2+x+1$$

$$A_2(x)=q_1(x)q_2(x)+1=x^3+x^2+x+1$$

$$B_{-1}(x)=1,\quad B_0(x)=0$$

$$B_1(x)=1,\quad B_2(x)=q_2(x)=x$$

因此，式（3-4）告诉我们

$$x(x^5+x^3+x+1)+(x^3+x^2+x+1)(x^3+x^2+x+1)=x+1$$

并且的确有

$$\deg x<\deg(x^3+x^2+x+1)<\deg(x^5+x^3+x+1)$$

作为欧几里德算法的直接应用，下面我们介绍最大公约数的若干重要性质。

今后，我们用符号

$$a\mid b\quad (a(x)\mid b(x))$$

表示 a 整除 b（$a(x)$ 整除 $b(x)$），而用符号

$$a\nmid b\quad (a(x)\nmid b(x))$$

表示 a 不能整除 b（$a(x)$ 不能整除 $b(x)$）。

定理3.1.6 （1）若 $r\mid a$，$r\mid b$，则 $r\mid(a,\ b)$。

（2）设m为任意正整数，则

$$(am,\ bm)=m(a,\ b) \tag{3-9}$$

（3）设r为a和b的公约数，则

$$\left(\frac{a}{r},\ \frac{b}{r}\right)=\frac{1}{r}(a,\ b) \tag{3-10}$$

特别

$$\left(\frac{a}{(a,\ b)},\ \frac{b}{(a,\ b)}\right)=1 \tag{3-11}$$

（4）若$(a,\ b)=1$，则

$$(ac,\ b)=(c,\ b) \tag{3-12}$$

证明 （1）由定理3.1.5即得。

（2）因为$(a,\ b)=Aa+Bb$

进而有

$$m(a,\ b)=Ama+Bmb$$

因此

$$(am,\ bm)|m(a,\ b)$$

另一方面，由于$(a,\ b)|a$，故有$m(a,\ b)|am$。同理，$m(a,\ b)|bm$。因此，由（1）得

$$m(a,\ b)|(am,\ bm)$$

注意到两个互相整除的正整数一定相等，故式（3-9）成立。

（3）由（2）得

$$(a,\ b)=\left(r\cdot\frac{a}{r},\ r\cdot\frac{b}{r}\right)=r\left(\frac{a}{r},\ \frac{b}{r}\right)$$

此即式（3-10）。置$r=(a,\ b)$，即得式（3-11）。

（4）因为$(ac,\ b)|ac$，$(ac,b)|bc$，故由（1）得，$(ac,\ b)|(ac,\ bc)$。由（2）得，$(ac,\ bc)=c(a,\ b)=c$。因此，$(ac,\ b)|c$。显然，$(ac,\ b)|b$，故再由（1）得

$$(ac,\ b)|(c,\ b)$$

另一方面，由$(c,\ b)|ac$，$(c,\ b)|b$，根据（1）得

$$(c,\ b)|(ac,\ b)$$

因此，式（3-12）成立。 〈证毕〉

对于多项式，相应的结果是完全相同的。我们就不再多费笔墨了。

定义3.1.2 设 a，b 为整数，若整数M能同时被 a 和 b 整除，则称M为 a，b 的一个公倍数，其中最小的正公倍数称为**最小公倍数**，记为 $[a, b]$。

定理3.1.7 $ab=(a, b)[a, b]$ (3-13)

证明 设$M=ak$为 a，b 的任意一个公倍数，则$\frac{M}{b}=\frac{ak}{b}$必为整数。令 $(a, b)=d$，$a=a_1d$，$b=b_1d$，我们有

$$\frac{ak}{b}=\frac{a_1dk}{b_1d}=\frac{a_1k}{b_1}$$

由式（3-11），$(a_1, b_1)=1$。我们証明，$b_1|k$。

事实上，因 $b_1|a_1k$，则由式（3-12）得

$$b_1=(a_1k, b_1)=(k, b_1)$$

这表明 $b_1|k$。今设 $k=b_1t$，则

$$M=ak=ab_1t=a\frac{b}{d}t=\frac{ab}{d}t \quad (3\text{-}14)$$

反之，任何形如式（3-14）的整数也是 a 和 b 的公倍数。因此，式（3-14）可视为 a 与 b 的公倍数的一般表达式。

特别，令 $t=1$，即得式（3-13）。〈证毕〉

推论3.1.7.1 两个整数的任意公倍数皆为它们的最小公倍数的倍数。

证明 结合式（3-13）和式（3-14）得

$$M=[a, b]t$$

〈证毕〉

对于多项式的情形，代替最小公倍数的是最低公倍式的概念，其相应的结论是完全类似的。

以下讨论整数的素因子标准分解这一重要问题。

设 p 为大于 1 的正整数，若除 1 和 p 外，p 不再有任何其它的约数，则称 p 为素数。不为素数且大于 1 的正整数称为合数。1 既不是素数也不是合数。

引理3.1.1 设 p 为素数。若 $p|ab$，则 $p|a$ 或 $p|b$。

证明 设 $p \nmid a$，则 $(p, a)=1$。由定理3.1.5，存在整数 M，N，使

$$Mp+Na=1$$

于是，

$$Mpb+Nab=b$$

因为 $p|Mpb$，$p|Nab$，故 $p|b$。〈证毕〉

引理3.1.2 设 p，q 为任意素数。于是，$p|q$ 当且仅当 $p=q$。

证明 若 $p|q$，则因 q 除 1 及 q 外不再有任何其它约数，故 $p=q$。

反之，若 $p=q$，显然有 $p|q$。〈证毕〉

定理3.1.8 任何大于 1 的整数 N 恒可分解为素因子的乘积；并且若不计诸因子的次序，则这种分解还是唯一的。

证明 我们先作一个声明：今后凡提及的约数，均指正约数。

设 p_1 是 N 的大于 1 的最小约数，则显然 p_1 为素数。置 $N=p_1N_1$，若 $N_1=1$，则分解完毕。若 $N_1>1$，则设 p_2 是 N_1 的最小素约数，即 $N_1=p_2N_2$。余此类推。由于

$$N>N_1>N_2>\cdots\geqslant 1$$

此项手续不能超过 N 次，故必到某一 $N_n=1$ 而停止。于是

$$N=p_1N_1=p_1p_2N_2=\cdots=p_1p_2\cdots p_nN_n=p_1p_2\cdots p_n$$

现在证明分解的唯一性。假如另有 N 的素因子分解式

$$N=q_1q_2\cdots q_r$$

则有

$$p_1p_2\cdots p_n=q_1q_2\cdots q_r \tag{3-15}$$

由于 $p_1|p_1p_2\cdots p_n$，则 $p_1|q_1q_2\cdots q_r$。根据引理3.1.1，p_1 必整除 q_1，…，q_r 之一，不妨设 $p_1|q_1$。根据引理 3.1.2，$p_1=q_1$。将式 (3-15) 两边同时约去 $p_1=q_1$，则有

$$p_2 \cdots p_n = q_2 \cdots q_r$$

余此类推。最后，等式的一边，例如左边，约掉了所有的因子。此时右边的因子也应该被全部约掉。如不然，则有

$$1 = q_{n+1} \cdots q_r$$

但是，$q_{n+1} \cdots q_r > 1$，故上述等式不能成立。　　〈证毕〉

在上述定理中，所得到的素因子分解中，将相同的素因子集中起来，并按素因子由小到大的次序排列，即得

$$N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \tag{3-16}$$

其中　$p_1 < p_2 < \cdots < p_k$，$e_i > 0$（$i = 1, \cdots, k$）

称式（3-16）为整数N的**标准分解式**。

利用整数的标准分解式，易求最大公约数和最小公倍数。

例3.1.2　求（150，42）和〔150，42〕。

由于

$$150 = 2^1 \cdot 3^1 \cdot 5^2 = 2^1 \cdot 3^1 \cdot 5^2 \cdot 7^0$$

$$42 = 2^1 \cdot 3^1 \cdot 7^1 = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^1$$

因此

$$(150, 42) = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 6$$

$$[150, 42] = 2^1 \cdot 3^1 \cdot 5^2 \cdot 7^1 = 1050$$

显然

$$150 \times 42 = 6300 = (150, 42)[150, 42] = 6 \times 1050$$

在多项式理论中，与整数论中素数的概念相平行的是所谓既约多项式的概念。

定义 3.1.3　设$f(x)$为次数大于零的多项式。若$f(x)$除常数及常数与$f(x)$的乘积外别无其它因式，则称$f(x)$为（在所讨论的范围内的）**既约多项式**。

注意，多项式的既约性与所讨论的范围有密切关系。例如

$$f(x) = x^2 + 1$$

在实数范围内（指多项式的系数取实数值）是既约多项式，但在

复数范围内就不是既约多项式了。因为此时有

$$f(x)=x^2+1=(x+i)(x-i)$$

由定义可见，多项式 $f(x)$ ($\deg f>0$) **是既约多项式当且仅当 $f(x)$ 不能分解为两个次数低于 $\deg f$ 的多项式之积。**

一个直接的推论是：**一次多项式在任何域上都是既约多项式。**

类似于引理 3.1.1，3.1.2 和定理3.1.3，对于既约多项式也有下述相应的引理和定理。

引理3.1.3 设 $f(x)$ 为既约多项式，$g_1(x)$，$g_2(x)$ 为任意多项式。于是，若 $f(x)|g_1(x)g_2(x)$，则 $f(x)|g_1(x)$ 或 $f(x)|g_2(x)$。

证明 类似于引理3.1.1。略。

引理3.1.4 设 $f(x)$，$g(x)$ 为两个首一既约多项式。于是，$f(x)|g(x)$ 当且仅当 $f(x)=g(x)$。

证明 若 $f(x)|g(x)$，则 $g(x)=cf(x)$。此处因 $g(x)$ 为既约多项式，故 c 为常数。又因 $f(x)$ 和 $g(x)$ 皆为首一多项式，故 $c=1$。因此，$f(x)=g(x)$。

反之，若 $f(x)=g(x)$，显然有 $f(x)|g(x)$。

〈证毕〉

定理3.1.9 任意首一多项式 $f(x)$ 恒可分解为既约多项式之乘积；若不计诸因式之次序则这种分解还是唯一的。

证明 若 $f(x)$ 为既约多项式，则已分解完毕。否则 $f(x)$ 可以分解为更低次的因式乘积。余此类推。因多项式的次数不可能无止境地低下去，所以最后一定可将 $f(x)$ 分解为首一既约多项式之乘积。

利用引理3.1.3和3.1.4，仿照定理3.1.8中的证法，可以完全类似地证明分解的唯一性。 〈证毕〉

在上述定理中所得到的既约因式分解中，将相同的既约因式集中起来，即得多项式的标准分解式：

$$f(x)=p_1^{e_1}(x)p_2^{e_2}(x)\cdots p_k^{e_k}(x)$$
$$e_i>0,\quad i=1,\ 2,\ \cdots,\ k \tag{3-17}$$

显然，一般多项式的标准分解式为

$$f(x)=c_n p_1^{e_1}(x)p_2^{e_2}(x)\cdots p_k^{e_k}(x)$$
$$e_i>0,\quad i=1,\ 2,\ \cdots,\ k \tag{3-18}$$

其中 c_n 是 $f(x)$ 的首项系数。

定理 3.1.9 的一个重要推论是

定理3.1.10 d 次多项式的一次因式不可能多于 d 个。

证明 设 $f(x)$ 为 d 次多项式，且有 $d+1$ 个一次因式，则由定理3.1.9，得

$$f(x)=(x+\alpha_1)(x+\alpha_2)\cdots(x+\alpha_{d+1})\cdot h(x)$$

其中 $h(x)$ 是其余既约因式的乘积。但上述等式右边之次数至少为 $d+1$，故产生矛盾。因此定理得证。 〈证毕〉

定理3.1.11 $f(\xi)=0$（即 ξ 为 $f(x)$ 的一个根）当且仅当 $(x-\xi)|f(x)$。

证明 由欧几里德除法，$f(x)$ 可写为

$$f(x)=(x-\xi)q(x)+r$$

其中 r 为常数。因此，$f(\xi)=0$ 当且仅当 $r=0$ 当且仅当 $(x-\xi)|f(x)$。 〈证毕〉

为完整起见，我们再引入两个定理，其中有关域和扩域的概念后面将详细讨论。

定理3.1.12 设 $f(x)$ 是域 F 上的 d 次多项式，则 $f(x)$ 在 F 的任何扩域上至多有 d 个根。

证明 设 $f(x)$ 有多于 d 个根，则由定理3.1.11，$f(x)$ 有多于 d 个一次因式，此与定理3.1.10矛盾。 〈证毕〉

众所周知，对于任意域 F 上的多项式

$$f(x)=c_nx^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0$$

对 $f(x)$ 求导，得

$$f'(x)\triangleq nc_nx^{n-1}+(n-1)c_{n-1}x^{n-2}+\cdots+c_1$$

有关导数的四则运算公式在这里仍然适用。

如果 $g^k(x)|f(x)$，但 $g^{k+1}(x)\nmid f(x)$，则称 $g(x)$ 为 $f(x)$ 的 **k重因式**。

定理3.1.13 设域F上的既约多项式 $p(x)$ 是 $f(x)$ 的 k 重因式，则$p(x)$ 必为 $f'(x)$ 的 $k-1$ 重因式。

证明 假设

$$f(x)=p^k(x)g(x)$$

其中$p(x)\nmid g(x)$。于是

$$f'(x)=p^{k-1}(x)[kp'(x)g(x)+p(x)g'(x)]$$

现只需证明

$$p(x)\nmid kp'(x)g(x)$$

假设不然，则因 $(p(x),\ g(x))=1$，我们有

$$\begin{aligned}p(x)&=(p(x),\ kp'(x)g(x))\\&=(p(x),\ kp'(x))\end{aligned}$$

因此，$p(x)|p'(x)$。由于 $\deg p'<\deg p$，这是不可能的。

〈证毕〉

综合上面的讨论不难看出，多项式的理论与整数的理论是完全平行的。多项式相当于整数，既约多项式相当于素数，而作为零次多项式的常数则相当于整数中的1，即它既不是既约多项式，也不是可约多项式。

§3.2 群和有限群

群是一种最重要的具有一种代数运算的集合。

定义3.2.1 设G是一个非空集合，其中定义了一种代数运算“$\cdot$”，并具有下述性质：

（1）（封闭性）若a，$b\in G$，则$a\cdot b\in G$；

（2）（结合律）若a，b，$c\in G$，则

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c$$

（3）G中（至少）存在一个（左）单位元素e，使得对一切$a\in G$，恒有

$$e \cdot a = a$$

（4）对G中任意元素a，（至少）存在一个（左）逆元素a^{-1}，使得

$$a^{-1} \cdot a = e$$

则称G（在所指定的代数运算之下）是一个群。

今后，在不致引起混淆的场合，我们常把群中的代数运算符号"·"省略不写，即把$a \cdot b$写成ab。

群具有下述重要性质。

首先，从定义可以推出，**左逆元素同时也是右逆元素。**

设$a \in G$，由（2），（3）及（4）得

$$a^{-1} a a^{-1} = ea^{-1} = a^{-1}$$

两端同时左乘a^{-1}的一个左逆元素，则有

$$eaa^{-1} = e$$

因此

$$aa^{-1} = e$$

其次，可以证明**左单位元素同时也是右单位元素。**

由（2）及（4）得

$$ae = a(a^{-1}a) = (aa^{-1})a$$

因为　$aa^{-1} = e$，

所以　$ae = ea = a$

进一步还有，**单位元素是唯一的。**

设e'也是G的单位元，则有

$$e = ee' = e'$$

同样可以推出，**逆元素也是唯一的。**

设b也是a的逆元素，则

$$\begin{aligned} a^{-1} &= a^{-1}e = a^{-1}(ab) = (a^{-1}a)b \\ &= eb = b \end{aligned}$$

综上所述，对于群中的单位元素及逆元素，非但不必有左、右之分，而且还进一步断定了它们的唯一性。因此，今后恒用e表示群G中的单位元素，用a^{-1}表示群G中元素a的逆元素。

最后，从等式

$$aa^{-1}=e$$

我们断定 a 也是 a^{-1} 的逆元素，即

$$(a^{-1})^{-1}=a$$

同时，不难得出

$$(ab)^{-1}=b^{-1}a^{-1}$$

事实上，

$$(b^{-1}a^{-1})(ab)=b^{-1}(a^{-1}a)\,b=b^{-1}eb=b^{-1}b=e$$

定义3.2.2 如果在群G中定义的代数运算满足交换律，即对任意a，$b\in G$，恒有

$$ab=ba$$

则称G为**交换群，或阿贝尔（Abel）群。**

例3.2.1 所有实数的集合在普通加法运算之下构成阿贝尔群。此处，相当于单位元素是0，任意实数a的逆元素是$-a$。

除零以外的全体实数在通常乘法运算之下也构成阿贝尔群。此处，单位元素是1，任意实数$a\neq 0$的逆元素是a^{-1}。

所有正、负整数及0的集合在通常加法运算之下构成阿贝尔群。但是，关于通常的乘法运算它并不构成群，因为0及每一个不等于1的整数都没有乘法逆元素。

例3.2.2 全体非奇异$n\times n$方阵的集合关于矩阵的乘法运算构成群，但不是阿贝尔群，因为矩阵的乘法运算不满足交换律。此处，单位元素是单位方阵，任意非奇异方阵的逆元素是它的逆方阵。

例3.2.? 平面上围绕一个固定点的一切旋转的集合也构成群。不过这个群中的元素不是数，而是一个确定的旋转。两个旋转α与β的乘积定义为先作旋转α再作旋转β，所得到的$\alpha\cdot\beta$仍是一个旋转。设p为平面上任意一点，$p\alpha$表示经过旋转α后所得到的点。结合率显然成立，因为

$$p\alpha(\beta\gamma)=(p\alpha)(\beta\gamma)=((p\alpha)\,\beta)\,\gamma$$

$$p\,(\alpha\beta)\,\gamma=(\,p\,(\alpha\beta))\,\gamma=((p\alpha)\,\beta)\,\gamma$$

即

$$\alpha(\beta\gamma)=(\alpha\beta)\gamma$$

旋转群的单位元素是旋转角度为 0° 的旋转。对于任意转角为 α° 的旋转，其逆元素为转角是 $-\alpha^\circ$ 的旋转。

上述例题引出了变换群的重要概念。所谓集合M的一个变换，是指由M到其自身的一个一一对应。M上全体变换的集合构成一个群，称为**变换群**。它的单位元素是恒等变换，记为 I。对任意 $a\in M$，恒有

$$aI=a$$

设 S 为集合M的一个变换，则其逆变换 S^{-1} 是具有下述性质的变换

$$S^{-1}S=I$$

显然，若 S 将 $a\in M$ 变为 $b\in M$，则 S^{-1} 将 b 变为 a。至于结合率，可像旋转群中一样地证明。

如果集合$M=\{a_1, a_2, \cdots, a_n\}$是一个由 n 个元素组成的有限集合，则M上的变换称为**置换**。集合M上全体变换（置换）的集合所构成的群称为 **n 次置换群**，记为 S_n。集合M的一部分置换所成的群称为**置换群**。

M上的置换可以写成

$$\begin{pmatrix} a_1 & a_2\cdots a_n \\ a_{i_1} & a_{i_2}\cdots a_{i_n} \end{pmatrix}$$

或进一步简写为

$$\begin{pmatrix} 1 & 2\cdots n \\ i_1 & i_2\cdots i_n \end{pmatrix}$$

例如，考虑两个 3 次置换

$$S_1=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\quad S_2=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

因为

$$1S_1=1,\quad 2S_1=3,\quad 3S_1=2$$

$$1S_2=2,\ 2S_2=1,\ 3S_2=3$$

所以

$$S_1S_2=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},\quad S_2S_1=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

可见，$S_1S_2\neq S_2S_1$。这表明，置换群不一定是阿贝尔群。因此，变换群不一定是阿贝尔群。但是不难看出，旋转群是阿贝尔群。

下面，我们讨论群的另一种定义。设性质（5）为

设 a，$b\in G$，则方程

$$ax=b \text{ 和 } ya=b$$

在G中皆有解。

定理3.2.1 设G是非空集合，则性质（1），（2），（3），（4）和（1），（2），（5）等价。

证明 设（1），（2），（3），（4）成立，则以 $x=a^{-1}b$ 代入方程$ax=b$得

$$a(a^{-1}b)=(aa^{-1})b=eb=b$$

同理可证，ba^{-1} 是方程 $ya=b$ 的解。

反之，设（1），（2），（5）成立。设$c\in G$，并将方程$yc=c$的一个解记为e，即$ec=c$。现在证明e即为G中的单位元素。事实上，对任意$a\in G$，设方程$cx=a$在G中之解为x_0，即$cx_0=a$。于是，

$$ea=e(cx_0)=(ec)x_0=cx_0=a$$

其次，由（5），对于任意$a\in G$，方程

$$xa=e$$

可解，其解自然是a^{-1}。〈证毕〉

这样，我们得到另一个关于群的完全等价的定义。

定义3.2.3 设G是一个非空集合，如果G具备性质（1），（2）和（5），则称G是一个群。

定理3.2.2 设G是群，则它一定具有性质

（6）（消去律）（i）设$ax=ax'$，则$x=x'$；（ii）设$ya=y'a$，则$y=y'$。

证明 （i）在 $ax=ax'$ 中两端左乘 a^{-1}，即得 $x=x'$。(ii) 同理可证。〈证毕〉

这一定理说明，方程 $ax=b$ 和 $ya=b$ 在群G中的解是唯一的。例如，x_1，$x_2\in G$，且 $ax_1=b$，$ax_2=b$，则 $ax_1=ax_2$。因此，$x_1=x_2$。

定义3.2.4 元素个数有限的群称为**有限群**。元素的个数称为该有限群的**阶**。

定理3.2.3 设G为非空有限集合，则性质（1），（2），（3），（4）和（1），（2），（6）等价。

证明 设G适合（1），（2），（3），（4），则G是有限群。由定理3.2.2，G必适合（6）。

反之，设（1），（2），（6）成立。我们只需证明（5）也成立。设a，$b\in G$，且设

$$G=\{a_1,\ a_2,\ \cdots,\ a_n\}$$

置
$$G'=\{aa_1,\ aa_2,\ \cdots,\ aa_n\}$$

由（1），$G'\subseteq G$。在集合G与G'之间建立对应

$$a_i\to aa_i,\quad i=1,\ 2,\ \cdots,\ n$$

由（6），当 $i\neq j$ 时，$aa_i\neq aa_j$。因此，上述对应是G到G'上的一一对应。但是，有限集合不可能与其真子集建立一一对应。于是，$G=G'$。因此，必有某个$a_k\in G$，适合 $aa_k=b$，即方程 $ax=b$ 在G中有解。同理可证，方程 $ya=b$ 也在G中有解。

〈证毕〉

注意，上述定理对无限集合并不成立。例如全体非零整数的集合，关于乘法虽然满足（1），（2），（6），但并不构成群。

有限群则不同。我们有，**非空有限集合G为有限群当且仅当G适合条件（1），（2），（6）**。

在编码理论中所涉及到的群都是有限群，因此，我们必须对它予以充分注意。

例3.2.4 显然，$GF(2)$ 关于加法构成二阶有限阿贝尔群。并且，$GF(2)$ 上的 n 维向量空间V_n构成阶为 2^n 的有限

阿贝尔群。而V_n的k维子空间，即二元（n，k）码，则构成阶为2^k的有限阿贝尔群。

例3.2.5 S_n是$n!$阶的有限群。因为n个元素的排列（不允许重复）共有$n!$个，每一个排列刚好相当于一个n次置换。

下面，我们阐述一种有用的观点。因为方程

$$ax=b$$

在群中有唯一的解$a^{-1}b$，我们可以视之为a与b"相除之商"，并且记为$\frac{b}{a}$。因而可以说，群中任意两个元素相除之商也在这个群中。这样一来，**在群中不但定义了一种封闭的代数运算，同时还由此相伴地导出了与之互逆的另一种封闭的代数运算。**

当考虑的群是阿贝尔群时，常常把其中的代数运算记成加法。此时单位元素记作0，因为它有普通数0一样的特性，对于任意$a\in G$，恒有$a+0=a$。其次任意$a\in G$的逆元素记作$-a$，满足$a+(-a)=0$。同时我们常常把$a+(-b)$记作$a-b$，这就是加法逆运算——减法。

最后，我们介绍一种重要的阿贝尔群——剩余类群。

定义3.2.5 设整数a和b除以同一正整数m时有相同的余数，即

$$a=a_1m+r,\quad b=b_1m+r,\quad 0\leqslant r<m$$

则称a和b关于模m同余，记为

$$a\equiv b\ (\mathrm{mod}\, m)$$

例如，$25\equiv 1\ (\mathrm{mod}\ 8)$，$16\equiv -5\ (\mathrm{mod}\ 7)$

由定义显然可见

$a\equiv b\ (\mathrm{mod}\, m)$ 当且仅当$a-b=mt$（即$m|(a-b)$）。

根据同余的概念，我们可以把全体整数加以分类。我们用自然数m去除全体整数，将余数为r的整数算作一类。这一类中的整数可以表示为

$$a=qm+r,\quad 0\leqslant r<m$$

的形式。当q遍历一切整数时，我们就得到这一类（记作$\bar{r}$）的

全体整数。

如此，我们将全体整数按模m分成m个类：

$$\bar{0},\ \bar{1},\ \bar{2},\ \cdots,\ \overline{m-1}$$

其中每一类都称作模m的一个剩余类。如果从每一类中各取一个整数作为代表，则称这些代表的全体为**模 m 的一个完全剩余系**。

剩余类中的任意整数都称作该剩余类的一个剩余。剩余类r中的数

$$a=qm+r,\quad 0\leqslant r<m$$

对应于$q=0$者刚好为r。因此，称r为剩余类$\bar{r}$的非负最小剩余。

模运算有下述重要性质。

定理3.2.4 若$a_1\equiv b_1\pmod m$，$a_2\equiv b_2\pmod m$，则

(1) $a_1+a_2\equiv b_1+b_2\pmod m$

(2) $a_1-a_2\equiv b_1-b_2\pmod m$

(3) $a_1\cdot a_2\equiv b_1\cdot b_2\pmod m$

证明 由定义可直接推出。

设$\bar{i}$，$\bar{j}$是模m的两个剩余类。我们定义整数$i+j$所代表的类$\overline{i+j}$为类$\bar{i}$与类$\bar{j}$之和，记为

$$\bar{i}+\bar{j}=\overline{i+j}$$

由定理3.2.4可知，如此定义的类$\overline{i+j}$并不因从类$\bar{i}$和类$\bar{j}$中所取之代表而改变，它仅与类$\bar{i}$及类$\bar{j}$本身有关。同样可定义类$\bar{i}$与类$\bar{j}$之乘积为$i\ j$所代表的类$\overline{ij}$，记为

$$\bar{i}\cdot\bar{j}=\overline{ij}$$

定理3.2.5 模m的全体剩余类集合关于剩余类加法运算构成m阶阿贝尔群。

证明 显然，剩余类加法满足结合律

$$(\bar{i}+\bar{j})+\bar{k}=\bar{i}+(\bar{j}+\bar{k})$$

及交换律

$$\bar{i}+\bar{j}=\bar{j}+\bar{i}$$

其次 $\bar{0}$是剩余类的加法单位元素，并且任意类$\bar{i}$的加法逆元素

为$-\bar{i}=\overline{m-i}$。 〈证毕〉

下面的定理是很有用的，今后我们会多次用到。

定理3.2.6 若$ac\equiv bc \pmod m$，且$(c,\ m)=1$，则

$$a\equiv b \pmod m$$

证明 由假设，$m|(a-b)c$。但$(c,\ m)=1$，故有

$$m=(m,\ (a-b)c)=(m,\ a-b),$$

即$m|(a-b)$。 〈证毕〉

这一定理表明，在同余式两边可以消去与模互素的公约数。从剩余类乘法运算的角度，这一定理可叙述成下述形式。

定理3.2.7 设$\bar{a}$，$\bar{b}$，$\bar{c}$是模m的三个剩余类。若$(c,m)=1$，则由$\bar{a}\cdot\bar{c}=\bar{b}\cdot\bar{c}$可推得$\bar{a}=\bar{b}$。

受这一定理的启发，我们可以尝试在模m的全体剩余类中找出一部分剩余类使其构成乘法群。

引理3.2.1 在模m的任意剩余类中，所有整数皆与m有相同的最大公约数。

证明 设$\bar{r}$为模m的任意一个剩余类，且设a_1，$a_2\in\bar{r}$。于是$a_1\equiv a_2 \pmod m$，即$a_1-a_2=mt$。因此$(a_1,\ m)=(a_2,\ m)$。由$(a_1,\ m)|a_1$，$(a_1,\ m)|m$得$(a_1,\ m)|a_2$。从而$(a_1,m)|(a_2,m)$。同理，$(a_2,\ m)|(a_1,\ m)$。 〈证毕〉

设n为正整数，**欧拉函数$\varphi(n)$**定义为与n互素且不大于n的正整数的个数，即

$$\varphi(n)\triangleq|\{a\,|\,0<a\leqslant n,\ (a,\ n)=1\}|$$

例如，当$n=6$时，只有1和5是小于6且与6互素的正整数。因此$\varphi(6)=2$。关于欧拉函数，以后还要详细讨论。

定理3.2.8 模m的剩余类中所有与m互素的剩余类的集合关于剩余类乘法构成$\varphi(m)$阶的有限阿贝尔群。

证明 设$\bar{a}$，$\bar{b}$是模m的两个与模m互素的剩余类，由于

$$(ab,\ m)=(b,\ m)=1$$

故$\bar{a}\cdot\bar{b}=\overline{ab}$亦为与$m$互素的剩余类。因此封闭性条件满足。

其次，在这一集合中剩余类乘法的交换律和结合律是成立的。

剩余类$\bar{1}$属于这个集合（因为（1，m）＝1），且显然为单位元素。现只需证明逆元素存在。由（a，m）＝1，存在整数A，M，使

$$Aa+Mm=1$$

写成同余式的形式，即

$$Aa\equiv 1 \pmod m$$

或

$$\overline{Aa}=\overline{A}\cdot\overline{a}=\bar{1}$$

下面我们证明，（$\overline{A}$，m）＝1，即（A，m）＝1。因为(参看引理3.2.1的证明)

$$(Aa,\ m)=(m,\ 1)$$

所以

$$(Aa,\ m)=(A,\ m)=1$$

从而$\overline{a}^{-1}=\overline{A}$。 〈证毕〉

§3.3 循 环 群

设H是群G的非空子集。如果H关于G中所定义的代数运算也构成群，则称H为群G的一个子群。

下面的定理指出群中子集构成子群的条件。

定理3.3.1 群G的非空子集H构成群当且仅当

（1）若$a\in H$，$b\in H$，则$ab\in H$

（2）若$a\in H$，则$a^{-1}\in H$

证明 必要性显然，只证充分性。群定义中的条件（1），（2），（4）显然满足。因为

$$aa^{-1}=e\in H$$

所以（3）也成立。 〈证毕〉

特别，若H是G的非空有限子集，则定理3.3.1中的条件（2）也是多余的。因为，此时可用条件（6）代替（3）和（4），而（4）对群G成立，自然对H也成立。因此，条件（1），（2）和（6）对H成立。综上所述，我们有

定理3.3.2　群G的非空有限子集H构成有限子群当且仅当若a，$b\in H$，则$ab\in H$。

定理3.3.1中的两个条件可以合并为一个条件。

定理3.3.3　群G的非空子集H构成群当且仅当若a，$b\in H$，则$ab^{-1}\in H$。

证明　必要性显然，只证充分性。设$a\in H$，令$b=a$，则$e=aa^{-1}\in H$。其次，由$e\in H$，$a\in H$，得$a^{-1}=ea^{-1}\in H$。最后，由a，$b\in H$（从而$b^{-1}\in H$）可得$a(b^{-1})^{-1}=ab\in H$。因此，H构成群。〈证毕〉

下面，我们介绍对编码理论十分重要的一类群——循环群。

定义3.3.1　由元素g及其幂构成的群G称为**循环群**，该元素g称作循环群G的**生成元**。

注意到

$$g^a g^b=g^{a+b}=g^b g^a$$

因此，**凡循环群都是阿贝尔群**。

例3.3.1　考虑复数域上的n次方程

$$z^n-1=0$$

如所周知，它在复数域上的全部根（称作n次单位根）的集合是$U_n=\{e^{\frac{2k\pi}{n}i}, k=0,1,\cdots,n-1\}$。显然，$U_n$构成群。令$\varepsilon=e^{\frac{2\pi}{n}i}$，则$U_n$是以$\varepsilon$为生成元的$n$阶有限循环群。以后我们将看到，只要$(n, s)=1$，则$\varepsilon^s$也是$U_n$的生成元。

例3.3.2　整数集合关于加法运算所构成的群是以1为生成元的无限循环群。在加法群中，对应于a^n的是

$$na=\underbrace{a+a+\cdots+a}_{n\text{个}}$$

对应于a^{-n}的是

$$-na=\underbrace{(-a)+(-a)+\cdots+(-a)}_{n\text{个}}$$

对应于a^0的是0，即加法群中的单位元素。

现在我们进一步研究循环群的构造。

设a为群G中的一个固定元素，可能会有两种情况。

（1）a的所有的幂都互不相同，这时以a为生成元的循环群

$$\{\cdots a^{-2},\ a^{-1},\ a^0=e,\ a^1,\ a^2,\ \cdots\}$$

是无限循环群。

（2）存在整数$i>j$，使$a^i=a^j$。于是

$$a^{i-j}=e,\quad i-j>0$$

这表明存在正整数$i-j$，使$a^{i-j}=e$。我们称满足

$$a^n=e$$

的最小正整数为**元素a的阶**。在情况(1)中，这种正整数不存在，此时称a为**无限阶元素**。

若a为n阶元素，则

$$a^0=e,\ a^1,\ a^2,\ \cdots,\ a^{n-1} \qquad (3\text{-}19)$$

互不相同。如果

$$a^i=a^j,\quad 0\leqslant j<i\leqslant n-1$$

则有

$$a^{i-j}=e$$

但是，$0<i-j\leqslant n-1$，此与a为n阶元素的假定矛盾。更进一步，我们断定在这种情况下，a的一切幂均已包含在序列(3-19)之中。设a^m为a的任意一个幂。m可写为

$$m=nq+r,\quad 0\leqslant r<n$$

因为$a^n=e$，所以有

$$a^m=a^{nq+r}=(a^n)^q a^r=a^r$$

因为$0\leqslant r<n$，所以$a^m=a^r$必在序列(3-19)之中。

综上所述，下述定理成立。

定理3.3.4 群G中的任意元素a皆能生成一个循环群，它是G的子群。如果a是无限阶元素，则a生成无限循环群。如果a是n阶元素，则a生成n阶循环群。

下面，我们讨论群中元素阶的性质。

定理3.3.5 设 a 为 n 阶元素，则

$a^m=e$ 当且仅当 $n|m$

证明 m 可以写成

$$m=qn+r,\quad 0\leqslant r<n$$

设 $a^m=e$，则

$$a^m=a^{qn+r}=(a^n)^q a^r=a^r=e$$

因为 a 是 n 阶元素，故 $r=0$，所以 $n|m$。

反之，设 $n|m$，则 $m=qn$。于是 $a^m=a^{qn}=(a^n)^q=e$。〈证毕〉

定理3.3.6 设 a 为 n 阶元素，b 为 m 阶元素，且 $(n,\ m)=1$，则 ab 为 mn 阶元素。

证明 因为所考虑的群是阿贝尔群，故

$$(ab)^{mn}=\underbrace{(ab)(ab)\cdots(ab)}_{mn\text{个}}=a^{mn}b^{mn}$$

$$=(a^n)^m(b^m)^n=e^m e^n=e$$

设 ab 之阶为 k，则由定理3.3.5，$k|mn$。

反之，由 $(ab)^k=e$ 得，$a^k=b^{-k}$，故 $a^{mk}=b^{-mk}=(b^m)^{-k}=e$。因此 $n|mk$。但因 $(n,\ m)=1$，故有

$$n=(n,\ mk)=(n,\ k)$$

即 $n|k$。同理，我们有 $b^{nk}=e$，因而 $m|k$。这表明 k 为 m，n 的一个公倍数。但因 $(m,\ n)=1$，故 $[m,\ n]=mn$。所以，$mn|k$。定理得证。〈证毕〉

定理3.3.7 设 a 为 n 阶元素，则 a^k 为 $\frac{n}{(k,\ n)}$ 阶元素。

证明 设 a^k 为 m 阶元素。因为

$$(a^k)^{\frac{n}{(k,\ n)}}=(a^n)^{\frac{k}{(k,\ n)}}=e$$

故 $m\left|\frac{n}{(k,\ n)}\right.$。

另一方面，由 $a^{km}=(a^k)^m=e$ 可知，$n|km$。因此 km 是 n，k 的一个公倍数。由推论3.1.7.1可知，

$$km=[k,\ n]\ t=\frac{kn}{(k,\ n)}t$$

即 $m=\frac{n}{(k,\ n)}t$。因此$\frac{n}{(k,\ n)}|m$。 〈证毕〉

推论3.3.7.1 设 a 为kn阶元素，则a^k为 n 阶元素。

证明 由定理3.3.7，a^k之阶为

$$\frac{kn}{(k,\ kn)}=\frac{kn}{k}=n$$ 〈证毕〉

设G为由元素 a 生成的 n 阶循环群，即

$$G=\{a^0=e,\ a^1,\ a^2,\ \cdots,\ a^{n-1}\}$$

根据定理3.3.7，我们可以计算出G中任意元素a^k之阶为$\frac{n}{(k,\ n)}$。显然a^k为 n 阶元素当且仅当$(n,\ k)=1$。因此 n 阶有限循环群G中共有$\varphi(n)$个 n 阶元素，其中$\varphi(n)$是欧拉函数。并且，G中每一个 n 阶元素都是G的生成元。

定义3.3.2 n 阶循环群G中任意 n 阶元素都称作G的**本原元**，或称作**n次单位原根**。相应地，称G中的m阶元素为**m次单位根**。

由上述讨论可知，n 阶循环群中任意生成元皆为本原元，这种元素共有$\varphi(n)$个。

例如，G为由元素 a 生成的 6 阶循环群

$$G=\{a^0=1,\ a^1,\ a^2,\ a^3,\ a^4,\ a^5\}$$

G中共有$\varphi(6)=2$个本原元（生成元），即a^1和a^5，它们都是 6 阶元素。其余的元素 1，a^2，a^3和a^4的阶分别为 1，3，2和3。注意，1，2和3都是6的约数。以后我们将看到，这个性质具有一般性。

鉴于循环群的概念在编码理论中的重要位置，在结束本节之前，我们还要讨论如何从已知的循环群找出它的全部子群的问题。

定理3.3.8 设G为由元素 a 生成的无限循环群，且H是G的子群。于是H仍为循环群。此外H或者是仅由单位元素构成的

有限群，或者是仅由具有最小可能的正指数m的元素a^m所生成的无限循环群。并且对于任意正整数m，由a^m所生成的循环群必为（群G的）无限子群。

证明 若H仅由单位元素构成，则定理已证。

若H不是仅由单位元素构成的群，则H中一定含有幂次为正整数的元素a^m。若$a^{-m}\in H$，则$(a^{-m})^{-1}=a^m\in H$。设a^m是H中具有最小可能的正指数m的元素，显然H包含a^m的任意次幂$(a^m)^k=a^{mk}$，其中k为整数。现在证明，H中的一切元素都是a^m的幂。设$a^s\in H$，由

$$s=qm+r,\quad 0\leqslant r<m$$

我们有

$$a^r=a^{s-qm}=a^s\cdot(a^m)^{-q}\in H$$

由m的选择，$r=0$，故$s=qm$，即$a^s=(a^m)^q$。因此H是由a^m生成的循环群。但是a为无限阶元素，故a^m也是无限阶元素，这表明H是无限循环群。〈证毕〉

由定理3.3.8可知，一个无限循环群$G=\langle a\rangle$的全部子群可列出如下：

$$\langle a^0=e\rangle,\ \langle a^1\rangle,\ \langle a^2\rangle,\ \cdots,\ \langle a^n\rangle,\ \cdots$$

定理3.3.9 设G为由元素a生成的n阶有限循环群，H是它的子群。于是

（1）H仍为有限阶循环群，它或者仅由单位元素构成，或者由具有最小可能的正指数m的元素a^m所生成；

（2）这种最小正指数m必为n的一个因子，并且子群H的阶数为$q=\dfrac{n}{m}$；

（3）对于n的任意正整数因子m，G中必有一个且仅有一个阶数为$q=\dfrac{n}{m}$的循环子群。

证明 （1）证明类似于定理3.3.8。

（2）由欧几里德除法

$$n = qm + r, \quad 0 \leqslant r < m$$

因此

$$a^r = a^{n-qm} = a^n(a^m)^{-q} = (a^m)^{-q} \in H$$

由 m 的取法，$r = 0$，即 $n = qm$。所以，a^m 的阶为

$$\frac{n}{(m, n)} = \frac{n}{m} = q$$

（3）设 m 为 n 的任意一个正整数因子，则由 a^m 可以生成 G 的一个阶数为 $q = \frac{n}{m}$ 的循环子群 H。现在证明，H 是 G 中唯一的 $q = \frac{n}{m}$ 阶子群。设 H' 为 G 的另一个 $q = \frac{n}{m}$ 阶子群，则它应当由 H' 中具有最小可能的正指数 m' 的元素 $a^{m'}$ 生成，且 $m' | n$。置 $n = q'm'$，则因 H' 为 q 阶群，故 $\frac{n}{m} = q = q' = \frac{n}{m'}$。因此 $m = m'$，即 $a^m = a^{m'}$。于是，$H = H'$。　　　　〈证毕〉

如果用 $\tau(n)$ 表示正整数 n 的正整数因子的个数，则由上述定理可知，n 阶有限循环群的任意子群都是阶数为 n 的约数的循环群，并且 n 阶循环群共有 $\tau(n)$ 个子群。

例如，$G = \{a^0, a^1, a^2, a^3, a^4, a^5\}$ 是 6 阶循环群，它的 $\tau(6) = 4$ 个循环子群是

$$\langle a_0 = e\rangle, \quad \langle a^3\rangle, \quad \langle a^2\rangle, \quad \langle a^1\rangle$$

1 阶　　2 阶　　3 阶　　6 阶

§3.4　陪集与正规子群

线性码的译码原理是根据整个空间 V_n 按其码向量空间 V_k 加以分类而建立起来的。实际上，空间 V_n 关于向量加法构成一个群，而子空间 V_k 是它的一个子群。因此本节讨论利用子群将整个群进行分类的问题，借以加深对于线性分组码理论的理解。

定义3.4.1　设 H 是群 G 的一个子群，$a \in G$，将 a 与子群 H 中的每一个元素相乘（不妨称群 G 中定义的代数运算为乘法），就得到形如 ah（$h \in H$）的元素的集合，记为 aH。称此集合为**子群 H 在群 G 中的一个左陪集**。

由定义不难看出，当 $a\in H$ 时，则有 $aH=H$。因此子群 H 本身也是一个左陪集。同样，若 $b\in aH$，即 $b=ah(h\in H)$，则 $bH=ahH=a(hH)=aH$。这表明左陪集 aH 可由其中任意一个元素唯一地确定。

类似地可以定义右陪集。如果讨论的群是阿贝尔群，则左陪集与右陪集是一致的。在编码理论中所遇到的群大都是阿贝尔群。

例3.4.1 设 Z 表示由全体整数构成的加法群，M 表示所有 m 的倍数所成的集合，其中 m 为正整数。显然 M 是 Z 的子群。设 $\bar{i}$ 为模 m 的一个剩余类，即

$$\bar{i}=\{i+mt,\quad t=0,\ \pm 1,\ \pm 2,\ \cdots\}$$

因而 $\bar{i}$ 实际上是子群 M 的一个陪集，即

$$\bar{i}=i+M$$

这样一来，所谓全体整数 Z 按模 m 分成 m 个类

$$\bar{0},\ \bar{1},\ \bar{2},\ \cdots,\ \overline{m-1}$$

实际上就是按子群 M 分成 m 个陪集

$$M,\ 1+M,\ 2+M,\ \cdots,\ (m-1)+M$$

在这个意义上，我们也把同余式

$$a\equiv b\ (\mathrm{mod}\, m)$$

记成

$$a\equiv b\ (M)$$

下面我们讨论陪集的一些性质。

引理3.4.1 元素 a，b 属于 H 的同一个陪集当且仅当 $b^{-1}a\in H$。

证明 设 a，b 属于 H 的同一个陪集，则 $a=bh(h\in H)$，从而 $b^{-1}a=h\in H$。

反之，若 $b^{-1}a\in H$，令 $h=b^{-1}a$，则 $a=bh$，即 a，b 属于 H 的同一个陪集。〈证毕〉

由这个引理可见，两个陪集 aH 与 bH 或者相等，或者互不相交。若 $aH\neq bH$，且 aH 与 bH 含有公共元素 c，即 $c=ah_1=$

$bh_2(h_1, h_2 \in H)$，则 $b^{-1}a = h_2h_1^{-1} \in H$。由引理 3.4.1，$aH = bH$，与假设矛盾。这样一来，引理 3.4.1 可改写成如下形式：

两个陪集 aH 与 bH 相等当且仅当 $b^{-1}a \in H$。

注意到加法群中相当于 $b^{-1}a$ 的是 $a - b$。因此引理3.4.1显然是§3.2中关于同余式的下述性质的推广：

$a \equiv b \pmod{m}$ 当且仅当 $a - b = mt$

如果令子群 H 中的每一个元素 h 与陪集 aH 中的元素 ah 对应

$$h \to ah$$

则这一对应是集合 H 与 aH 之间的一一对应。若 $ah \in aH$ 除 h 外还对应 H 中的元素 h'，则由 $ah = ah'$ 得，$h = h'$

如果两个集合之间能建立某种一一对应的关系，则称这两个集合是等势的。对于有限集合，两个集合等势意味着两个集合所含的元素个数相等。

由此可见，群 G 可以利用它的子群 H 进行分类，使群 G 被划分成一系列等势的陪集。在这些陪集中，除子群 H 以外，其余的陪集都不是群。若 $aH \neq H$，则 $a \notin H$，于是 $e \notin aH$。否则若 $e = ah(h \in H)$，则 $h = a^{-1}e = a^{-1} \in H$，从而 $a \in H$，矛盾。因此 aH 不是群。

现在我们根据上述思想对编码理论中具有重要意义的有限群作进一步研究。

设 G 为 N 阶有限群，H 是 G 的 n 阶子群：

$$H = \{g_1, g_2, \cdots, g_n\}$$

于是，有限群 G 按子群 H 被划分成有限个陪集，每个陪集中都含有 n 个元素。假定这样的陪集共有 j 个，把它们排列如下：

$a_1H(a_1 = e)$：	g_1	g_2	g_3	$\cdots$	g_n
a_2H：	a_2g_1	a_2g_2	a_2g_3	$\cdots$	a_2g_n
$\cdots$	$\cdots$				
a_jH：	a_jg_1	a_jg_2	a_jg_3	$\cdots$	a_jg_n

像第二章一样，我们也称上述阵列为**标准阵列**。

由于群 G 中含有 N 个元素，我们有

$$N = nj$$

由此推出下述著名的拉格朗日（Lagrange）定理。

定理3.4.1（拉格朗日定理） 有限群中子群的阶数是整个群的阶数的约数。

称有限群G由子群H所分成的陪集的个数j为**子群H在群G中的指数**。

由拉格朗日定理可以得到许多重要的结论。

若命H为由G中元素g所生成的循环群，则由定理3.3.4，g所生成的循环群H的阶数即为元素g的阶数。因此得

定理3.4.2 在有限群中，任意元素的阶都是这个有限群的阶数的约数。

由此直接推得，在n阶有限群中，任意元素a均满足等式

$$a^n = e$$

设a为m阶元素，由上述定理，$m \mid n$，即$n = mq$，于是

$$a^n = a^{mq} = (a^m)^q = e$$

作为例子，我们指出定理3.4.2在数论中的应用。

由定理3.2.8，与模m互素的剩余类全体G构成$\varphi(m)$阶有限群。设$\bar{a}$是与m互素的一个剩余类，即$(a, m) = 1$。又假设$\bar{a}$作为G中的元素，$\bar{a}$的阶为k。因此根据定理3.4.2，$k \mid \varphi(m)$。由定理3.3.5，我们有

$$\bar{a}^{\varphi(m)} = \bar{1}$$

因此

$$\overline{a^{\varphi(m)}} = \bar{1}$$

这就是数论上著名的欧拉（Euler）定理。

定理3.4.3（欧拉定理） 设$(a, m) = 1$，则

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

今后我们将证明，若m的标准分解式为$m = p_1^{e_1} \cdots p_k^{e_k}$，则欧拉函数有如下公式：

$$\varphi(m) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

特别，命 m 为素数 p，即得

$$\varphi(p)=p\left(1-\frac{1}{p}\right)=p-1$$

因此，我们获得下述著名的费马（Fermat）定理，它是欧拉定理的一种特殊形式。

定理3.4.4 （费马定理） 设 p 为素数，且 $(a, p)=1$，则

$$a^{p-1}\equiv 1 \pmod p$$

若$\bar{a}$的阶为 k，则 k 为满足等式$\bar{a}^k=\bar{1}$的最小正整数，亦即 k 为满足同余式$a^k\equiv 1 \pmod m$ 之最小正整数($(a, m)=1$)。称 k 为**a关于模m的方次数，或称为a关于模m的阶。**

在此，我们作一个注记。模m的全部剩余类的集合以及与模m互素的剩余类集合，分别关于加法和乘法构成有限群。前者之阶为m，后者之阶为$\varphi(m)$。并且模m的全部剩余类

$$\{\bar{0}, \bar{1}, \bar{2}, \overline{m-1}\}$$

还是m阶循环加法群，其生成元素为$\bar{1}$。但是，与模m互素的剩余类集合所成的$\varphi(m)$阶有限群却不一定是循环群。例如，与模 8 互素的剩余类集合

$$\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$$

是 4 阶有限乘法群，但不是循环群。事实上，

$$\bar{1}^2=\bar{1},\ \bar{3}^2=\bar{1},\ \bar{5}^2=\bar{1},\ \bar{7}^2=\bar{1}$$

所以，这个群没有生成元。而与模 9 互素的剩余类集合

$$\{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$$

则是循环群的例子，它以$\bar{2}$为生成元。

上述事实表明，**有限群不一定是循环群。**

关于以多项式为模的剩余类的概念也可以类似地加以定义，并且有与本节内容相应的结果。关于这一点，我们今后还会谈到。

与陪集有关的是群论中的另一个重要概念，即所谓正规子群的概念。

定义3.4.2 设H为群G的子群。如果子群H的每一个左陪集也是H的右陪集，即对于任意$a\in G$，恒有

$$aH=Ha$$

则称H为群G的**正规子群，或不变子群**。

下面的定理可以用来验证一个子群是否是正规子群，其中（4）尤为方便。

定理3.4.5 设H是群G的子群，则下述4个命题是彼此等价的

（1）H是群G的正规子群；

（2）对任意$a\in G$，恒有$aHa^{-1}=H$

（3）对任意$a\in G$，恒有$aHa^{-1}\subseteq H$

（4）对任意$a\in G$及任意$h\in H$，恒有 $aha^{-1}\in H$

证明 证明的步骤是：（1）⇒（2）⇒（3）⇒（4）⇒（1），从而4个条件等价。

（1）⇒（2） 对任意$a\in G$，由（1）得，$aH=Ha$。因此$aHa^{-1}=(aH)a^{-1}=(Ha)a^{-1}=H(aa^{-1})=He=H$。

（2）⇒（3） 显然。

（3）⇒（4） 对任意$a\in G$及任意$h\in H$，由（3）得，$aha^{-1}\in H$。

（4）⇒（1） 对任意$ah\in aH$，由于$aha^{-1}\in H$，即$aha^{-1}=h_1$ $(h_1\in H)$，故得$ah=h_1a$。因此，$aH\subseteq Ha$。另一方面，对任意$ha\in Ha$，由于$a^{-1}ha\in H$，同理可得$Ha\subseteq aH$。于是对任意$a\in G$恒有$aH=Ha$。 〈证毕〉

例3.4.2 设 $G=\left\{\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}\middle|\ r\neq 0,\ s\text{是有理数}\right\}$

则G关于矩阵乘法构成一个群。设

$$H=\left\{\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\middle|\ t\text{为有理数}\right\}$$

则H是群G的一个正规子群。事实上

$$\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} r & s \\ 0 & 1 \end{pmatrix}^{-1}=\begin{pmatrix} r & rt+s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} r^{-1} & -r^{-1}s \\ 0 & 1 \end{pmatrix}$$

$$=\begin{pmatrix} 1 & rt \\ 0 & 1 \end{pmatrix}\in K$$

因此由定理3.4.5之（4），H是正规子群。

推论3.4.5.1 阿贝尔群的任意子群都是正规子群。

证明 设H是阿贝尔群G的子群。于是，对任意$a\in G$及任意$h\in H$，我们有

$$aha^{-1}=haa^{-1}=h\in H$$

因此，H是G的正规子群。〈证毕〉

显然，由正整数m的一切倍数所成的集合M，是整数加法群Z的正规子群。模m的剩余类集合关于剩余类加法之所以能够成为群，其决定性因素就在于M是Z的正规子群。作为这一结果的一般化，就导致了下述定理，它充分显示了正规子群的作用。

定理3.4.6 若H为群G的正规子群，则H的全体陪集必构成群。

证明 首先需要定义陪集之间的乘法运算。设$\bar{a}=aH$，$\bar{b}=bH$为两个陪集，我们定义以ab为代表元的陪集，$\overline{ab}=(ab)H$为陪集aH与bH的乘积，即

$$\bar{a}\cdot\bar{b}=\overline{ab}$$

这一定义的合理性可如下证明。设$a_1\in aH$，$b_1\in bH$，即

$$a_1=ah_1,\ b_1=bh_2,\ h_1,\ h_2\in H$$

则

$$a_1b_1=(ah_1)(bh_2)=a(h_1b)h_2$$

由于H是正规子群，故

$$h_1b=bh_3,\ h_3\in H$$

因此

$$a_1b_1=a(bh_3)h_2=(ab)(h_3h_2)\in(ab)H$$

亦即

$$(a_1b_1)H=(ab)H$$

其次证明结合律成立。事实上

$$(\bar{a}\bar{b})\bar{c}=\overline{ab}\,\bar{c}=\overline{abc}$$

$$\bar{a}(\bar{b}\bar{c})=\bar{a}\,\overline{bc}=\overline{abc}$$

故得

$$(\bar{a}\bar{b})\bar{c}=\bar{a}(\bar{b}\bar{c})$$

设 e 为群 G 的单位元素。因为

$$\bar{e}\bar{a}=\overline{ea}=\bar{a}$$

所以 $\bar{e}=eH=H$ 是陪集集合的单位元素。

最后，任意陪集 $\bar{a}=aH$ 的逆元素为 $\overline{a^{-1}}=a^{-1}H$。事实上

$$\bar{a}\overline{a^{-1}}=\overline{aa^{-1}}=\bar{e}$$

定理得证　　　　　　　　　　　　　　　　　　　　（证毕）

例3.4.3　设 Z 为整数加法群，M 为由 5 的一切倍数所构成的集合，则 M 是 Z 的正规子群。于是，Z 按子群 M 被分成 5 类，排列如下：

$\bar{0}=M$ ：	0	5	-5	10	-10	15	$-15\cdots$
$\bar{1}=1+M$：	1	6	-4	11	-9	16	$-14\cdots$
$\bar{2}=2+M$：	2	7	-3	12	-8	17	$-13\cdots$
$\bar{3}=3+M$：	3	8	-2	13	-7	18	$-12\cdots$
$\bar{4}=4+M$：	4	9	-1	14	-6	19	$-11\cdots$

由定理3.4.6，M 的 5 个陪集

$$\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},\ \bar{4}$$

关于剩余类加法构成群，这是一个 5 阶阿贝尔群，其运算见表 3-1。

表　3-1

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

由此可见，我们从更加一般的角度重新得到了定理3.2.5。

定义3.4.3 设H为群G的正规子群，称G的全体陪集所成的群为**G关于H的商群**，记为G/H。

设G为有限群，并用$|G|$表示G的阶数。于是，商群G/H的阶数是H在群G中的指数，亦即

$$|G/H|=\frac{|G|}{|H|}$$

这就是商群这一名称的来源。

§3.5 同构和同态

同构的概念是近代数学中最重要的思想之一。我们先从一个例子谈起。

例3.5.1 考虑下述二元（4，2）码C

$$(0000),\ (1001),\ (0111),\ (1110)$$

令C的每一个码字$(a_0,\ a_1,\ a_2,\ a_3)$都对应一个多项式$a_0+a_1x+a_2x^2+a_3x^3$($a_i=0$或1)。于是，在4个码字和4个二元多项式之间建立了下述一一对应的关系：

$$(0000)\leftrightarrow 0+0\cdot x+0\cdot x^2+0\cdot x^3=0\ (\text{零多项式})$$

$$(1001)\leftrightarrow 1+0\cdot x+0\cdot x^2+1\cdot x^3=1+x^3$$

$$(0111)\leftrightarrow 0+1\cdot x+1\cdot x^2+1\cdot x^3=x+x^2+x^3$$

$$(1110)\leftrightarrow 1+1\cdot x+1\cdot x^2+0\cdot x^3=1+x+x^2$$

不仅如此，在这个对应之下，与C中任意两个码字之和对应的多项式刚好等于这两个码字对应的多项式之和。例如，与码字(1001)及(0111)之和(1110)对应的多项式为

$$(1+x^3)+(x+x^2+x^3)=1+x+x^2$$

即

$$(1001)+(0111)\leftrightarrow(1+x^3)+(x+x^2+x^3)$$

不难看出，与码群C对应的多项式集合

$$0,\ 1+x^3,\ x+x^2+x^3,\ 1+x+x^2$$

关于多项式的加法运算也构成群。因此，我们可以把每一个码字

视为它对应的多项式，从而使我们有可能借助于多项式的理论来研究码字，这就把我们从线性码单纯地作为线性空间的局限中解放了出来。

定义3.5.1 设 f 是集合 A 到集合 B 的一个映射。对于任意 a，$b\in A$，如果 $a\neq b$，恒有 $f(a)\neq f(b)$，则称 f 是 A 到 B 的一个**单射**，或 A 到 B 内的**一一映射**。

对于任意 $b\in B$，如果恒有 $a\in A$，使

$$f(a)=b$$

则称 f 是 A 到 B 的一个**满射**，或 A 到 B **上的映射**。

如果 A 到 B 的映射 f 既是单射又是满射，则称 f 是 A 到 B 的一个**双射**，或 A 到 B **上的一一映射**。

为方便计，有时我们把定义了运算·的群 G 记为（G，·）。

定义3.5.2 设（G，·）和（$\overline{G}$，$*$）是两个群。如果存在 G 到 $\overline{G}$ 的一个双射 f，并且保持运算，即对于任意 a，$b\in G$，恒有

$$f(ab)=f(a)*f(b)$$

则称 f 是 G 到 $\overline{G}$ 上的同构映射，并称 G 和 $\overline{G}$ **同构**，记为 $G\cong\overline{G}$。

特别，当 $G=\overline{G}$ 时，则称所说的同构为**自同构**。

关于同构，我们有下面的重要定理。

定理3.5.1 设（G，·）$\cong$（$\overline{G}$，$*$），f 是同构映射。若 e 是 G 的单位元素，则 $f(e)$ 是 $\overline{G}$ 的单位元素。并且 $\overline{G}$ 中任意元素 $f(a)$ 的逆元素是 $f(a^{-1})$。

证明 首先，对任意 $f(a)\in\overline{G}$，恒有

$$f(a)*f(e)=f(ae)=f(a)$$

因此 $f(e)$ 是 $\overline{G}$ 的单位元。

其次我们有

$$f(a)*f(a^{-1})=f(aa^{-1})=f(e)$$

所以

$$f(a)^{-1}=f(a^{-1})$$

〈证毕〉

由此可见，同构映射把单位元素变为单位元素，把逆元素变

为逆元素。

不限于群，对于其它的代数系统，例如后面要讲的环与域等，也可以建立同构的概念。

在数学上，我们把同构的两个系统视为本质上完全相同的系统。可以说，同构的概念是近代数学中的卓越思想之一。它可以把表面上看来似乎毫不相干的事物从本质上找到内在的联系，从而使我们能够透过现象抓住事物的本质。

鉴于同构的重要性，我们举一些例子说明同构的应用。

首先我们证明，例3.3.1和例3.3.2实际上概括了所有的循环群。

定理3.5.2 设Z是整数加法群，G是无限循环群，则$G\cong Z$。

证明 设$G=\langle a\rangle$，命$f(a^k)=k$，我们证明f是G到Z的同构映射。

首先证明，f是映射，即对于任意$g\in G$，$f(g)$都是唯一确定的。由于$G=\langle a\rangle$是无限循环群，故a的不同方幂互不相同，因此，f是映射。

其次设$a^m\neq a^n$，则显然$m\neq n$，故f是单射。设$m\in Z$，则$a^m\in G$，且$f(a^m)=m$，因此f是满射。

由于

$$f(a^m\cdot a^n)=f(a^{m+n})=m+n=f(a^m)+f(a^n)$$

所以f保持运算。因此$G\cong Z$。 〈证毕〉

类似地，设$U_n=\langle\varepsilon\rangle$是如例3.3.1中所定义的$n$阶循环群，我们有

定理3.5.3 设G是n阶有限循环群，则$G\cong U_n$。

证明 设

$$G=\langle a\rangle=\{a^0=e,\ a^1,\ a^2,\ \cdots,\ a^{n-1}\}$$

命$f(a^k)=\varepsilon^k$，$k=0,1,\cdots,n-1$，则f显然是G到U_n的双射。

此外，对任意a^m，$a^n\in G$，恒有

$f(a^m \cdot a^n) = f(a^{m+n}) = \varepsilon^{m+n} = \varepsilon^m \cdot \varepsilon^n = f(a^m) \cdot f(a^n)$. 所以，$f$ 保持运算。因而，$G \cong U_n$。 〈证毕〉

上述两个定理表明，只要掌握了（Z，$+$）和（U_n，$\cdot$），就等于掌握了所有的循环群。

下面的定理是很有用的。

定理3.5.4 设（G，$\circ$）是一个群，$\overline{G}$ 是定义了代数运算"$*$"的集合。如果存在 G 到 $\overline{G}$ 的双射，且保持运算，即对任意 a，$b \in G$，恒有

$$f(a \circ b) = f(a) * f(b)$$

则（$\overline{G}$，$*$）也是一个群，且 $G \cong \overline{G}$。

证明 对任意 $f(a)$，$f(b)$，$f(c) \in \overline{G}$，恒有

$$\begin{aligned}(f(a) * f(b)) * f(c) &= f(a \circ b) * f(c) \\ &= f((a \circ b) \circ c) = f(a \circ (b \circ c)) \\ &= f(a) * f(b \circ c) = f(a) * (f(b) * f(c))\end{aligned}$$

即结合律成立。

类似于定理3.5.1，我们可以证明 $f(e)$ 是 $\overline{G}$ 的单位元素，其中 e 是 G 的单位元素。$f(a) \in \overline{G}$ 的逆元素是 $f(a^{-1})$。〈证毕〉

例3.5.2 考虑例3.4.3中的模5剩余类加法群 $Z/M \triangleq G$，以及它的加法表。U_5 的乘法表是

$\cdot$	1	ε	ε^2	ε^3	ε^4
1	1	ε	ε^2	ε^3	ε^4
ε	ε	ε^2	ε^3	ε^4	1
ε^2	ε^2	ε^3	ε^4	1	ε
ε^3	ε^3	ε^4	1	ε	ε^2
ε^4	ε^4	1	ε	ε^2	ε^3

显然，$G \cong U_5$。因为命

$$f: \quad f(\overline{k}) = \varepsilon^k, \quad k = 0, 1, 2, 3, 4$$

则 f 是 G 到 U_5 上的同构映射。此外，不难看出

$$\overline{0} \leftrightarrow 1, \quad \overline{1} \leftrightarrow \varepsilon$$

即循环群的生成元（单位元）的同构象仍为生成元（单位元），这

是具有一般性的。

对于任意群，我们有

定理3.5.5 （凯莱（Cayley））任意群G都和一个变换群同构。

证明 为方便计，我们认为两个变换的乘积是从右向左，即先作右边的变换，再作左边的变换。请读者注意。

任取$a \in G$，定义G的左乘变换如下

$$\pi_a: \pi_a(x) = ax, \text{ 对一切 } x \in G.$$

我们证明，π_a是G到G的一一变换。对任意$b \in G$，因方程$ax = b$在G中有解，故存在$x \in G$，使$\pi_a(x) = b$。因此，π_a是满射。其次，若$x \neq y$，则$ax \neq ay$。否则，由$ax = ay$，根据消去律将导致$x = y$，与假设矛盾。所以，π_a是单射。因而，π_a是一一变换。

因为$(\pi_a\pi_b)(x) = \pi_a(\pi_b(x)) = \pi_a(bx) = a(bx) = (ab)x = \pi_{ab}(x)$，故对一切$a$，$b \in G$，恒有$\pi_a\pi_b = \pi_{ab}$，即变换的乘积在$\overline{G} = \{\pi_a | a \in G\}$上是封闭的。

现在定义G到$\overline{G}$的映射

f：$f(a) = \pi_a$，对一切$a \in G$

显然，f是满射。若$f(a) = f(b)$，则$\pi_a = \pi_b$。设e是G中的单位元素，由$\pi_a(e) = \pi_b(e)$得$a = b$，故f是单射。因此，f是双射。

此外，f还保持运算。事实上

$$f(ab) = \pi_{ab} = \pi_a\pi_b = f(a)f(b)$$

因此，f是G到$\overline{G}$上的同构映射。由定理3.5.4，$\overline{G}$也是群，并且$G \cong \overline{G}$。 〈证毕〉

推论3.5.5.1 设G为n阶有限群，则G和S_n的一个子群同构。

证明 由定理3.5.5立得。

如此看来，变换群在群论中占有重要位置是不言而喻的。因为在同构的意义上，我们可以将任意群都视为一个变换群。同样

地，对于有限群，置换群的特殊作用也是毋庸置疑的。有鉴于此，下面我们进一步考察一下置换群。先从一个例子谈起。

例3.5.3 设

$$S_3=\{1, a, b, c, d, e\}$$

其中

$$1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad a=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$$b=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad c=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$d=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\quad e=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

a是2阶元素，因为

$$a^2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&3&2\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=1$$

类似地，b是2阶元素，c是3阶元素，等等。

下面我们给出S_3的乘法表。

·	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	1	d	e	b	c
b	b	c	1	a	e	d
c	c	b	e	d	1	a
d	d	e	a	1	c	b
e	e	d	c	b	a	1

由乘法表可见，S_3不是阿贝尔群，因而不是循环群，故没有6阶元素。事实上，S_3有一个1阶元素1（即单位元素），3个2阶元素a，b和e，以及2个3阶元素c和d。

我们常常把置换表示成循环的形式。例如$a=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$，

其中存在着形如 $2\ \rightleftarrows\ 3$ 的循环，我们称之为 S_3 中一个长度为 2 的循环，或简称为 2 —循环，并记为（2，3）。因此，S_3 中的元素的循环型为

$$1=(1),\quad a=(2,\ 3),\quad b=(1,\ 2)$$

$$c=(1,\ 2,\ 3),\quad d=(1,\ 3,\ 2),\quad e=(1,\ 3)$$

其中（1）是习惯记法，表示恒等置换。此外循环的记法不是唯一的。例如（1 2 3）=（2 3 1）=（3 1 2）

定义3.5.3 设 n 次置换 $\pi\in S_n$ 的形状如下：

$$\pi=\begin{pmatrix} a_1 & a_2\cdots a_i & a_{i+1}\cdots a_n \\ a_2 & a_3\cdots a_1 & a_{i+1}\cdots a_n \end{pmatrix}$$

则称 π 为一个 i —循环，并记作 $(a_1,\ a_2,\ \cdots,\ a_i)$

循环不仅记法简单，还有下述重要性质。

定理3.5.6 （1）S_n 中任意一个 i —循环都是 i 阶元素；

（2）$(a_1,\ a_2,\ \cdots,\ a_i)^{-1}=(a_i,\ a_{i-1},\ \cdots,\ a_2,\ a_1)$；

（3）不相交的循环乘积的因子可以交换次序；

（4）任意 n 次置换 π 都可以分解为有限个不相交的循环的乘积；

（5）设 $\pi\in S_n$ 分解成不相交循环的乘积 $\pi=\pi_1\pi_2\cdots\pi_k$，且 $\pi_1,\ \pi_2,\ \cdots,\ \pi_k$ 之阶分别为 $r_1,\ r_2,\ \cdots,\ r_k$，则 π 是 $[r_1,\ r_2,\ \cdots,\ r_k]$ 阶元素。

证明 （1），（2），（3）显然。

（4）考虑 $a_1,\ \pi(a_1),\ \pi^2(a_1),\ \cdots$，由于集合的有限性，上述序列必然出现重复，且第一次出现重复时必有 $\pi^i(a_1)=a_1$。否则存在 $k<j\leqslant i$，使得 $\pi^j(a_1)=\pi^k(a_1)$。因此 $\pi^{j-k}(a_1)=a_1$ 是更早出现的重复，与假设矛盾。于是，我们得到一个循环 $(a_1,\ \pi(a_1),\ \cdots,\ \pi^{i-1}(a_1))$。若 $i=n$，则（4）已证明。否则，任取一个不在此循环中的元素 b_1，依上法同样可以得到一个循环 $(b_1,\ \pi(b_1),\ \cdots,\ \pi^{j-1}(b_1))$。由上面的构造方法，这两个循环不可能

相交。假定不然，设 $\pi^r(a_1)=\pi^s(b_1)$ 是公共元素，$0\leqslant r\leqslant i-1$，$0\leqslant s\leqslant j-1$。不妨设 $r\geqslant s$，则 $\pi^{r-s}(a_1)=b_1$，因而 b_1 属于循环 $(a_1, \pi(a_1), \cdots, \pi^{i-1}(a_1))$，与假设矛盾。继续上述过程，直到将集合中的元素全部包括为止，最后得到

$$\pi=(a_1, \pi(a_1), \cdots, \pi^{i-1}(a_1))(b_1, \pi(b_1), \cdots, \pi^{j-1}(b_1))\cdots(f_1, \pi(f_1), \cdots, \pi^{p-1}(f_1))$$

因而（4）得证。

（5）设 π 是 m 阶元素，则由定理之（3）得

$$(1)=\pi^m=\pi_1^m\pi_2^m\cdots\pi_k^m$$

因为 π_1，π_2，…，π_k 互不相交，故

$$\pi_1^m=(1),\ \pi_2^m=(1),\ \cdots,\ \pi_k^m=(1)$$

因此

$$r_1|m,\ r_2|m,\ \cdots,\ r_k|m$$

即

$$[r_1, r_2, \cdots, r_k]|m$$

另一方面

$$\pi^{[r_1, r_2, \cdots, r_k]}=(1)$$

所以 $m=[r_1, r_2, \cdots, r_k]$。 〈证毕〉

例如 $(2, 3)(1, 3)=(1, 2, 3)$ 是3阶元素。而 $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 3 & 5 & 1 & 2 & 6\end{pmatrix}=(1, 4)(2, 3, 5)$ 是 $[2, 3]=6$ 阶元素。

我们再看一个同构的例子。

例3.5.4 设 $G=U_3=\{1, \varepsilon, \varepsilon^2\}$，其中 $\varepsilon=e^{\frac{2\pi}{3}i}$。我们证明 U_3 和 S_3 的一个子群同构。

仿照定理3.5.5，定义 G 的三个左乘变换如下：

$$\pi_1(x)=x,\ \pi_\varepsilon(x)=\varepsilon x,\ \pi_{\varepsilon^2}(x)=\varepsilon^2 x$$

其中，$x\in G=\{1, \varepsilon, \varepsilon^2\}$

亦即

$$\pi_1=\begin{pmatrix}1 & \varepsilon & \varepsilon^2\\ 1 & \varepsilon & \varepsilon^2\end{pmatrix},\quad \pi_\varepsilon=\begin{pmatrix}1 & \varepsilon & \varepsilon^2\\ \varepsilon & \varepsilon^2 & 1\end{pmatrix},\quad \pi_{\varepsilon^2}=\begin{pmatrix}1 & \varepsilon & \varepsilon^2\\ \varepsilon^2 & 1 & \varepsilon\end{pmatrix}$$

或用置换的循环型表示为

$$\pi_1=(1),\quad \pi_\varepsilon=(1,\ 2,\ 3),\quad \pi_{\varepsilon^2}=(1,\ 3,\ 2)$$

现在定义G到$\overline{G}$的同构映射

$$f(a)=\pi_a,\quad a=1,\ \varepsilon,\ \varepsilon^2$$

因而

$$G\cong\overline{G}=\{(1),(1,\ 2,\ 3),(1,\ 3,\ 2)\}\subseteq S_3$$

在本节的末尾，我们引入同态的概念。像同构一样，同态是研究群和一般代数系统的重要工具。

定义3.5.4 设f是群G到群$\overline{G}$的映射，如果f保持运算，即对任意a，$b\in G$，恒有

$$f(ab)=f(a)f(b)$$

则称f是G到$\overline{G}$的一个**同态映射**，简称**同态**。

若f为满射，则称f是G到$\overline{G}$的**满同态**，记为$G\sim\overline{G}$，并称$\overline{G}$是在f下G的**同态象**。

若f为单射，则称f是G到$\overline{G}$的**单同态**。

特别，当$G=\overline{G}$时，则称所说的同态为**自同态**。

因此，若f既是满同态又是单同态，则f是同构映射。可见同态扩展了同构的概念。

例3.5.5 设G和$\overline{G}$是两个群，e是$\overline{G}$中的单位元，则G到$\overline{G}$的映射

f：$f(a)=e$，对一切$a\in G$

保持运算，因为对任意a，$b\in G$恒有

$$f(ab)=e=f(a)f(b)$$

所以$f(G)=\{e\}$是G到$\overline{G}$的同态映射。

这是一种任意两个群之间都具有的同态。由于它把G的任意元都映射成零元（针对加法群而言），故常称之为**零同态**。

例3.5.6 设H是群G的正规子群，则

f：$f(a)=aH$，对一切$a\in G$

是G到G/H的满射，且保持运算，即对任意a，$b\in G$，恒有

$$f(ab)=(ab)H=(aH)(bH)=f(a)f(b)$$

因此f是G到G/H的满同态，并称之为**自然同态**。由此可见，任意群都和它的商群同态。不仅如此，我们还可以证明，若$G\sim\bar{G}$，则$\bar{G}$和G的某个商群同构。因此在同构的意义上，任意群的同态象都是它的商群。

例如，$G=S_3$，$H=\{(1),(1,2,3),(1,3,2)\}$

因为

（1） $H=H=H(1)$

(12) $H=\{(1,2),(2,3),(1,3)\}=H(1,2)$

所以H是G的一个正规子群。

设f是G到G/H的自然同态，则

$$f((1))=f((1,2,3))=f((1,3,2))=(1)H$$

$$f((1,2))=f((2,3))=f((1,3))=(1,2)H$$

§3.6 环与域

在编码理论中，为了更好地研究码字，单纯把码字的集合作为只有一种代数运算的体系就显得很不够了。我们希望码字的集合能够具有尽可能多的代数运算。这就是引入环和域这两个概念的目的。

定义3.6.1 设在非空集合R上定义了两种（封闭的）代数运算，分别记作“+”与“·”，并且满足下述条件

（1） R关于加法运算“+”构成阿贝尔群；

（2） R关于乘法运算“·”满足结合律，即对于任意a，b，$c\in R$，恒有

$$a(bc)=(ab)c$$

（3） 关于加法与乘法满足分配律，即对于任意a，b，$c\in R$，恒有

$$a(b+c)=ab+ac,\quad (b+c)a=ba+ca$$

则称R为**环**，且记为$(R,+,\cdot)$。

如果环R的子集合S关于R中的代数运算也构成环，则称S为R的**子环**，R为S的**扩环**。

如果环R关于乘法还满足交换律，即对于任意a，$b \in R$，恒有

$$ab=ba$$

则称R为**交换环**。

例3.6.1 整数集合Z关于普通的加法和乘法构成交换环，称为**整数环**，记作（Z，$+$，$\cdot$）。全体偶数的集合构成整数环的子环。

例3.6.2 模m的剩余类集合

$$\{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{m-1}\}$$

关于剩余类加法和剩余类乘法运算构成一个交换环，称之为**模m剩余类环**。

例3.6.3 阵元为实数的n阶方阵的全体关于方阵的加法与乘法运算构成环，称为实数上的**n阶方阵环**。但它不是交换环。例如，

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

有趣的是，在环中有许多与平常算术中不同的特性。

首先，一个环可以没有单位元素。所谓环R中的元素1是**单位元素**，是指对任意$a \in R$，恒有

$$1 \cdot a = a \cdot 1 = a$$

例如，偶数环是一个没有单位元素的环。

其次，环中的元素可能没有逆元素。设R是一个具有单位元素的环，对于$a \in R$，若存在$a^{-1} \in R$，使得

$$aa^{-1}=a^{-1}a=1$$

则称a^{-1}为a的**逆元素**。

例如，在整数环 Z 中，除 ± 1 有逆元素外，其余的整数都没有逆元素。

像乘法群一样，当环 R 有单位元素和逆元素时，它们都是唯一的。

最后，环中可能含有零因子。

定义3.6.2 设 a，$b \in R$，若 $a \neq 0$，$b \neq 0$，但 $ab = 0$，则称 a，b 是**零因子**。

例如，考虑模 8 剩余类环

$$\{\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},\ \bar{4},\ \bar{5},\ \bar{6},\ \bar{7}\}$$

由于 $\bar{2}\cdot\bar{4}=\bar{8}=\bar{0}$，故 $\bar{2}$ 和 $\bar{4}$ 是零因子。

又如在实数上的二阶方阵环中，由于

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

故等式左边的两个方阵都是零因子。

我们称不含零因子的交换环为**整环**。

在近世代数中，基本的代数系统除群、环以外，还有体和域。

定义3.6.3 我们称非空集合 R 为**体**，如果 R 是环，且满足下述条件

（1） R 中至少含有一个非零元素；

（2） R 中存在单位元素；

（3） R 中任意非零元素都有逆元素。

如果体 R 关于乘法运算还满足交换律，则称 R 为**域**。注意，这时 R 也是交换环。

由定义可见，体中全体元素关于加法构成阿贝尔加法群，体中全体非零元素关于乘法构成乘法群。因此可以说体是两个群的联合，并通过分配律互相联系。对域而言，这个乘法群还是阿贝尔乘法群。

与环不同，对于体和域，上述那些违反通常算术规律的现象

不复存在。

在体和域中都不含有零因子。设$a\neq 0$，而$ab=0$，则两边乘以a^{-1}得

$$a^{-1}(ab)=(a^{-1}a)b=1\cdot b=b=0$$

例3.6.4 全体有理数，全体实数，全体复数都构成域，分别称为**有理数域，实数域、复数域**。这些都是无限域的例子。

例3.6.5 由0，1两个元素构成的集合$GF(2)$是有限域的例子，称为**二元域**。它的加法单位元是0，乘法单位元是1。1的乘法逆元素即1本身。

例3.6.6 设p为素数，则模p剩余类集合

$$\{\bar{0},\ \bar{1},\ \bar{2},\ \cdots\overline{p-1}\}$$

构成域。由定理3.2.5，这个集合关于剩余类加法构成阿贝尔加法群。再由定理3.2.8，这个集合中的非零元素关于剩余类乘法构成阿贝尔乘法群。此外，分配律显然成立。因此剩余类集合$\{\bar{0},\ \bar{1},\ \cdots,\ \overline{p-1}\}$构成域，并记为$GF(p)$。

元素个数有限的域（体）称为**有限域（体）**。

已经证明，**有限体必为有限域**。因此，在有限集合的范围内，体和域可以不加区别。

有限域是编码理论中的基本工具，后面用一章的篇幅专门讨论。

下面介绍重要的多项式环。

考虑含有一个未定元的多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

其中系数a_i取自某一个域F，并用$F[x]$表示系数在F上的全体多项式的集合。

以前所讲的系数在实数域上的多项式的有关概念，可以毫不改变地平移过来。

定理3.6.1 $F[x]$按通常的加法和乘法构成具有单位元素的整环。

证明 $F[x]$显然构成阿贝尔加法群，零元素即零多项式。

$F[x]$中任意多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

的加法逆元素为

$$-f(x)=-a_0-a_1x-\cdots-a_nx^n$$

乘法结合律、交换律以及加法和乘法的分配律显然成立。因此，$F[x]$构成交换环。

其次域F中的单位元1作为多项式

$$1+0\cdot x+0\cdot x^2+\cdots+0\cdot x^n$$

就是$F[x]$的单位元素。

最后证明$F[x]$无零因子。设$f(x)\neq 0$，$g(x)\neq 0$，a_α、b_β分别是$f(x)$和$g(x)$的最高次项系数。于是$a_\alpha\neq 0$，$b_\beta\neq 0$。由于域F无零因子，故$a_\alpha b_\beta\neq 0$。但$a_\alpha b_\beta$是多项式$f(x)g(x)$的最高次项系数，因此$f(x)g(x)\neq 0$。〈证毕〉

域F上的多项式环$F[x]$最重要的性质是，在$F[x]$中欧几里德除法成立。换言之，对于任意$f(x)$，$g(x)\neq 0\in F[x]$，必定存在唯一的$q(x)$，$r(x)\in F[x]$，使得

$$f(x)=q(x)g(x)+r(x)$$

其中或者$r(x)=0$，或者$\deg r(x)<\deg g(x)$。

这样，前面讲到的关于整数的一切性质均可照搬到$F[x]$中来。多项式环与整数环是完全平行的，其原因就在于两者都是所谓**欧氏环**，即欧几里德除法成立的且有单位元的整环。

定义3.6.4 若$F[x]$中的两个多项式$a(x)$和$b(x)$被同一个多项式$f(x)$相除时有相同的余式

$a(x)=q_1(x)f(x)+r(x)$，$b(x)=q_2(x)f(x)+r(x)$ 则称$a(x)$，$b(x)$关于模$f(x)$同余，记为

$$a(x)\equiv b(x)\bmod f(x)$$

由定义易见，

$a(x)\equiv b(x)\bmod f(x)$ 当且仅当 $a(x)-b(x)=g(x)f(x)$，$g(x)\in F[x]$ （即$f(x)|a(x)-b(x)$）。

命 $\bar{a}(x)$ 表示 $F[x]$ 中与 $a(x)$ 关于模 $f(x)$ 同余的全体多项式的集合。像整数的情形一样，按照这种办法，$F(x)$ 中的全体多项式将被划分成剩余类。这些剩余类的全体所成之集合记为 $F[x]\bmod\bar{f}(x)$ 或 $F[x]\bmod f(x)$，并且不难证明

定理3.6.2 设 $f(x)\in F[x]$，且 $\deg f(x)>0$。于是，$F[x]\bmod\bar{f}(x)$ 构成具有单位元素的交换环，有时也记为 $F[x]/\bar{f}$ 或 $F[x]/f$。

多项式剩余类环 $F[x]/\bar{f}$ 在编码理论中占有极其重要的位置。

例3.6.7 考虑多项式环 $GF(2)[x]$。于是，

$$GF_2[x]\bmod(x^2+1)=\{\bar{0},\ \bar{1},\ \bar{x},\ \overline{x+1}\}$$

构成具有单位元的交换环，其运算表如下：

$+$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{1}$	$\overline{x+1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{x+1}$	$\bar{0}$

从上表可见，尽管 $\overline{x+1}\neq 0$，但是

$$\overline{x+1}\cdot\overline{x+1}=\bar{0}$$

因此，$\overline{x+1}$ 是多项式剩余类环 $GF(2)[x]/\overline{x^2+1}$ 中的零因子。由于 $\overline{x+1}^2=0$，有时也称类 $\overline{x+1}$ 为环中的**幂零元素**。

进一步，当 $f(x)$ 是域 F 上的既约多项式(自然 $\deg f>0$)时，我们有下述与例3.6.6相应的结果。

定理3.6.3 设 $f(x)$ 是域 F 上的既约多项式，则 $F[x]\bmod\bar{f}(x)$ 构成域。

证明 只需证明$F[x]\bmod \bar{f}(x)$中的任意非零元素均有乘法逆元素。设 $\bar{g}(x)\neq\bar{0}\in F[x]\bmod \bar{f}(x)$，则 $(g(x), f(x))=1$。由定理3.1.4，存在$a(x)$，$b(x)\in F[x]$，使

$$a(x)g(x)+b(x)f(x)=1$$

因此，

$$\overline{a(x)g(x)+b(x)f(x)}=\bar{a}(x)\bar{g}(x)+\bar{b}(x)\bar{f}(x)$$

$$=\bar{a}(x)\bar{g}(x)+\bar{b}(x)\cdot\bar{0}=\bar{a}(x)\bar{g}(x)=\bar{1}$$

这表明$\bar{a}(x)$是$\bar{g}(x)$的乘法逆元素。〈证毕〉

这一定理在构造有限域的模型中起着重要作用。

§3.7 理想、主理想和主理想环

理想是一种重要的子环，它在环论中的地位相当于正规子群在群论中的位置。在引入理想的概念之前，我们先给出一个构成子环的充分必要条件。

定理3.7.1 设N是环R中的非空子集合，则N为R的子环当且仅当

（1）N是R作为阿贝尔加法群的一个子群，即若a，$b\in N$，则$a-b\in N$；

（2）若a，$b\in N$，则$ab\in N$

证明 必要性显然成立，只证充分性。

由（1），N关于环R中的加法运算构成阿贝尔加法群。由（2），N关于环R中的乘法运算具有封闭性。此外，乘法结合律与分配律在R中成立，自然在N中也成立。因此，N是环。〈证毕〉

定义3.7.1 设N是交换环R的非空子集，如果

（1）由a，$b\in N$可以推出$a-b\in N$；

（2）由$a\in N$，$r\in R$可以推出$ar\in N$，

则称N是环R的一个理想。

由定义中之（1）可见，理想N是环R的加法子群。当$a\in N$，$r\in R$时，称ra为a的倍元素。因此，定义中之（2）说明，若$a\in N$，则a的一切倍元素也属于N。

显然，环R的理想必为环R的子环。因此，常称理想为理想子环。

一个非零环至少有两个理想。一个是仅由环中的零元素所构成的理想，称为零理想。另一个是R本身，称为单位理想。除此之外，如果R还有其它理想，则称为真理想。今后，我们只对真理想进行讨论。

例3.7.1　在整数环Z中，任意取定$m\in Z$，则$N=\{mn|n\in Z\}$是Z的理想。

例3.7.2　在域F上多项式环$F[x]$中，任意取定$f(x)\in F[x]$，则$N=\{g(x)f(x)|g(x)\in F[x]\}$是$F[x]$的理想。

建立了理想的概念以后，我们就可以把整数剩余类环和多项式剩余类环统一起来，得到所谓一般剩余类环。

设N是交换环R的理想，则N是环R的加法群（阿贝尔群）的正规子群。于是，R可按子群N划分成陪集，每一个陪集可写成$a+N$的形式，其中$a\in R$，或简记成$\bar{a}$。每个陪集也叫作一个剩余类。由定理3.4.6，这些陪集（剩余类）的全体构成阿贝尔加法群，记为$R \bmod N$。

若R中两个元素a，b属于同一个剩余类，则称a，b关于模N同余，记为

$$a\equiv b\ (\mathrm{mod} N)$$

由此不难得到

$a\equiv b\ (\mathrm{mod} N)$ 当且仅当$a-b\in N$。

事实上，若$a\equiv b\ (\mathrm{mod} N)$，则$a=b+n$，$n\in N$，即$a-b=n\in N$。反之，若$a-b\in N$，则$a=b+n$，$n\in N$，即$a\in b+N$。因此$a\equiv b\ (\mathrm{mod} N)$。

设$\bar{a}=a+N$，$\bar{b}=b+N$，定义剩余类$\overline{ab}=ab+N$为剩余类$\bar{a}$与$\bar{b}$的乘积

$$\bar{a}\bar{b}=\overline{ab}$$

这个定义是合理的。因为，设$a_1\in\bar{a}$，$b_1\in\bar{b}$，即

$$a_1 = a + n_1,\ b_1 = b + n_2,\ n_1,\ n_2 \in N$$

于是

$$a_1 b_1 = ab + (an_2 + bn_1 + n_1 n_2)$$

由于N为理想（注意，这是关键所在！），故

$$an_2 + bn_1 + n_1 n_2 \in N$$

因此 $a_1 b_1 \in ab + N$，即 $\overline{a_1 b_1} = \overline{ab}$。可见剩余类$\overline{ab}$并不因 $\bar{a}$，$\bar{b}$ 中代表元的选择而改变。

其次，因环R中的元素满足乘法结合律、交换律和分配律，故剩余类集合 $R\bmod N$也满足相应的规律。

以分配律为例。设 $\bar{a}$，$\bar{b}$，$\bar{c} \in R\bmod N$，则

$$\bar{a}(\bar{b}+\bar{c}) = \bar{a}\,\overline{(b+c)} = \overline{a(b+c)}$$

由于R中的元素满足分配律，即

$$a(b+c) = ab + ac$$

故有

$$\overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c}$$

因此

$$\bar{a}(\bar{b}+\bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$$

综上所述，我们有

定理3.7.2 设N为交换环R的理想，则 $R\bmod N$ 构成交换环，**称为环R以理想N为模的剩余类环**。

因此多项式剩余类集合和整数剩余类集合皆构成剩余类环就十分自然了。例 3.7.1 和 3.7.2 说明，一个整数的全体倍数和一个多项式的全体倍式都构成理想。

下面我们讨论在一个给定的环中，如何形成它的理想子环的问题。

设R是交换环，Z是整数环，任意取定 $a \in R$，则集合

$$\langle a \rangle \triangleq \{ra + na \mid r \in R,\ n \in Z\}$$

就是R的一个理想。设 $r_1 a + n_1 a \in \langle a \rangle$，$r_2 a + n_2 a \in \langle a \rangle$，则

$$(r_1 a + n_1 a) - (r_2 a + n_2 a) = (r_1 - r_2)a + (n_1 - n_2)a \in \langle a \rangle$$

设 $s \in R$，$ra + na \in \langle a \rangle$，则

$$s\,(ra+na)=sra+nsa=(sr+ns)\,a+0\cdot a$$

因为 $sr+ns\in R$，$0\in Z$，故 $s\,(ra+na)\in\langle a\rangle$。因此 $\langle a\rangle$ 为 R 的理想。称 $\langle a\rangle$ 为由**环 R 中元素 a 所生成的理想**。

显然 $\langle a\rangle$ 是环 R 中包含元素 a 的最小理想。事实上，环 R 中包含 a 的任意理想 N 必然包含一切 ra（r 取遍 R 中一切元素）及 $\pm(a+a+\cdots+a)=na$（$n\in Z$），从而也包含它们的和 $ra+na$。因此 $N\supseteq\langle a\rangle$。

请读者注意，关系式 $ra+na$ 切不可写成 $(r+n)\,a$，因为 $r\in R$，$n\in Z$，故 $r+n$ 没有意义。

然而当环 R 中有单位元素 e 时，则 $ra+na$ 可以写成下述形式：

$$ra+na=ra+nea=(r+ne)\,a=r'a$$

其中 $r'\in R$。因此在这种情形下，$\langle a\rangle$ 由 a 的一切倍元素组成。

例如，当 $R=Z$ 时，$\langle m\rangle=\{mn|\,n\in Z\}$。当 $R=F[x]$ 时，$\langle f(x)\rangle=\{g(x)f(x)|\,g(x)\in F[x]\}$（参看例 3.7.1 和例 3.7.2）。之所以如此，是因为整数环和多项式环皆为有单位元的环。在编码理论中所遇到的大多是这种环。

定义3.7.2 在交换环 R 中，由元素 $a\in R$ 所生成的理想 $\langle a\rangle$ 称为环 R 的一个**主理想**。称元素 a 为该主理想的**生成元素**。

定义3.7.3 设 R 是有单位元的交换环，如果

（1）环 R 无零因子；

（2）环 R 的每一个理想都是主理想；

则称环 R 为**主理想环**，记为 $P\ I\ R$。

定理3.7.3 整数环是主理想环。

证明 显然 Z 是有单位元的整环。我们只需证明 Z 的任何理想都是主理想。

设 N 为 Z 的任意理想。若 $N=\{0\}$，则 N 显然是主理想。否则，N 中必有一个最小的正整数 a（若 $c\neq 0\in N$，则 $-c\in N$，c 与 $-c$ 中必有一个正整数）。设 b 是 N 中任意元素，则由欧几里德除法

$$b = qa + r,\quad 0 \leqslant r < a$$

由理想的定义，$r = b - qa \in N$，因此 $r = 0$，即 $b = qa$。于是 $N = \langle a \rangle$。（证毕）

类似地，我们有

定理3.7.4 域 F 上的多项式环 $F[x]$ 是主理想环。

证明 类似于定理3.7.3。

$F[x]$ 中的理想 $\langle f(x) \rangle$ 的生成元 $f(x)$ 常称为**生成多项式**。若规定生成多项式为首一多项式时，则生成多项式是唯一的。

现在考虑多项式剩余类环 $F[x]/f(x)$。由例3.6.7可知，这种环是可能有零因子的。当 $f(x)$ 是可约多项式时，$f(x) = g(x)h(x)$，$\deg g > 0$，$\deg h > 0$，则 $\bar{f}(x) = \bar{0} = \bar{g}(x)\bar{h}(x)$，即 $\bar{g}(x)$ 和 $\bar{h}(x)$ 是零因子。这表明，当 $f(x)$ 可约时，剩余类环 $F[x]/f(x)$ 必有零因子。因此这种环不是主理想环。

如果放弃主理想环中的条件（1），则有

定理3.7.5 多项式剩余类环 $F[x]/f(x)$ 中的任意理想皆为主理想（$\deg f > 0$），并且该主理想的生成多项式必整除 $f(x)$。

证明 设 N 是 $F[x]/f$ 中的任意理想，若 $N = \{\bar{0}\}$，则显然 N 是主理想。否则存在 $\bar{a}(x) \neq \bar{0} \in N$。$N$ 中每一个类中都有一个次数最低的多项式作为该类的代表。设 $g(x)$ 是 N 的全部剩余类代表中次数最低的多项式。我们证明，$\bar{g}(x)$ 即为 N 的生成元素。若 $\bar{s}(x) \in N$，则

$$s(x) = q(x)g(x) + r(x),\quad \deg r < \deg g \text{ 或 } r(x) = 0$$

由此

$$\bar{s}(x) = \bar{q}(x)\bar{g}(x) + \bar{r}(x)$$

从而 $\bar{r}(x) = \bar{s}(x) - \bar{q}(x)\bar{g}(x) \in N$。由于 $g(x)$ 的取法，必有 $r(x) = 0$，即 $\bar{r}(x) = \bar{0}$。因此，$\bar{s}(x) = \bar{q}(x)\bar{g}(x)$，即 N 是主理想。

其次我们证明 $g(x) \mid f(x)$。由欧几里德除法

$$f(x)=q_1(x)g(x)+r_1(x),\quad \deg r_1<\deg g, \text{或 } r_1(x)=0$$

从而

$$0=\bar{f}(x)=\bar{q}_1(x)\bar{g}(x)+\bar{r}_1(x)$$

由于 $\bar{0}\in N$，故 $\bar{f}(x)-\bar{q}_1(x)\bar{g}(x)=\bar{r}_1(x)\in N$。根据 $g(x)$ 的取法，必有 $r_1(x)=0$。因此 $g(x)|f(x)$。〈证毕〉

称上述定理中的生成多项式 $g(x)$ 为理想 N 的生成多项式。当规定生成多项式是首一多项式时，它还是唯一的。若另有生成多项式 $g_1(x)$，则必有 $g_1(x)|g(x)$，$g(x)|g_1(x)$，即 $g_1(x)=g(x)$。

§3.8 代数、群代数、线性码的代数同构表示

在第二章所介绍的线性空间的概念中，作为纯量与空间中的元素乘积 αx，我们总是假定 α 是普通的数。如果假定这些纯量 α 取自任一域 F，类似地将得到所谓域 F 上的线性空间。第二章所介绍的全部线性空间的理论可以毫不改变地平移过来。

我们知道，线性空间中的元素（向量）构成阿贝尔加法群。如果还能定义该空间中元素之间的乘法，并使它构成环，就导致了所谓“代数”的概念。

定义3.8.1 设 V_n 为域 F 上的 n 维线性空间。若在 V_n 中还定义了乘法运算使 V_n 构成环，且满足

$$\lambda(xy)=(\lambda x)y=x(\lambda y)$$

其中 $x, y\in V_n$，$\lambda\in F$，则称 V_n 为域 F 上的一个秩为 n 的代数。

如果所定义的乘法还满足交换律，则称 V_n 为交换代数。

在编码理论中起重要作用的一种交换代数是多项式剩余类代数。

定理3.8.1 设 $f(x)$ 为域 F 上的 n 次多项式，则多项式剩余类 $F[x]\bmod f(x)$ 构成域 F 上秩为 n 的交换代数。

证明 对于 $\lambda\in F$，$\bar{a}(x)\in F[x]\bmod f(x)$，我们定义纯量 λ 与类 $\bar{a}(x)$ 的乘积为

$$\lambda\bar{a}(x)=\overline{\lambda a(x)}$$

现在证明这一定义的合理性。若 $a_1(x)\in\bar{a}(x)$，即 $a_1(x)=a(x)+g(x)f(x)$，从而 $\lambda a_1(x)=\lambda a(x)+\lambda g(x)f(x)$。因此，

$$\overline{\lambda a_1(x)}=\overline{\lambda a(x)+\lambda g(x)f(x)}=\overline{\lambda a(x)}+\overline{\lambda g(x)}\,\bar{f}(x)=\overline{\lambda a(x)}+\overline{\lambda g(x)}\cdot\bar{0}=\overline{\lambda a(x)}$$

可见，如此定义的乘积并不因类 $\bar{a}(x)$ 中代表多项式的选择而改变。

这样一来，$F[x]\bmod f(x)$就构成F上的n维线性空间了。n个剩余类

$$\bar{1},\ \bar{x},\ \bar{x}^2,\ \cdots,\ \overline{x^{n-1}}$$

构成$F[x]\bmod f(x)$的基底。因为$F[x]\bmod f(x)$的每一个非零类总有唯一的一个次数低于n的域F上的多项式作为代表，所以

$$\overline{a_0+a_1x+\cdots+a_{n-1}x^{n-1}}=\overline{a_0\cdot 1}+\overline{a_1x}+\cdots+\overline{a_{n-1}x^{n-1}}=a_0\cdot\bar{1}+a_1\cdot\bar{x}+\cdots+a_{n-1}\cdot\overline{x^{n-1}}$$

同样地

$$\bar{0}=0\cdot\bar{1}+0\cdot\bar{x}+\cdots+0\cdot\overline{x^{n-1}}$$

因此$F[x]\bmod f(x)$中的每一类皆可表示为这n个类$\bar{1}$，$\bar{x}$，…，$\overline{x^{n-1}}$的线性组合。其次这n个类还是线性独立的。若

$$a_0\cdot\bar{1}+a_1\cdot\bar{x}+\cdots+a_{n-1}\cdot\overline{x^{n-1}}=\bar{0}$$

则

$$a_0\cdot\bar{1}+a_1\cdot\bar{x}+\cdots+a_{n-1}\cdot\overline{x^{n-1}}=\overline{a_0+a_1x+\cdots+a_{n-1}x^{n-1}}=\bar{0}$$

但n次多项式$f(x)$应整除$a_0+a_1x+\cdots+a_{n-1}x^{n-1}$，故$a_0=a_1=\cdots=a_{n-1}=0$

此外我们有

$$\lambda(\bar{f}(x)\bar{g}(x))=\lambda\,\overline{f(x)g(x)}=\overline{\lambda f(x)g(x)}$$

$$(\lambda\bar{f}(x))\bar{g}(x)=\overline{\lambda f(x)}\,\bar{g}(x)=\overline{\lambda f(x)g(x)}$$

$$\bar{f}(x)(\lambda\bar{g}(x))=\bar{f}(x)\overline{\lambda g(x)}=\overline{f(x)\lambda g(x)}=\overline{\lambda f(x)g(x)}$$

因此

$$\lambda(\bar{f}(x)\bar{g}(x))=(\lambda\bar{f}(x))\bar{g}(x)=\bar{f}(x)(\lambda\bar{g}(x))$$

综上所述，$F[x]\bmod f(x)$ 是域F上秩为n的代数。由于$F[x]\bmod f(x)$ 是交换环，故这一代数还是交换代数。

（证毕）

若令$F=GF(2)$，$f(x)=x^n-1$，则得到域$GF(2)$上秩为n的交换代数$GF(2)[x]/x^n-1$。

现在假定V_n是$GF(2)$上的n维向量空间，我们在V_n与$GF(2)/x^n-1$之间建立一一对应的关系：

$$\boldsymbol{a}=(a_0,\ a_1,\ \cdots,\ a_{n-1})\longleftrightarrow\overline{a_0+a_1x+\cdots+a_{n-1}x^{n-1}}$$

为使V_n构成代数，我们需要定义V_n中向量之间的乘法。对于

$$\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})\longleftrightarrow\bar{a}(x)=\overline{a_0+a_1x+\cdots+a_{n-1}x^{n-1}}$$

$$\boldsymbol{b}=(b_0,b_1,\cdots,b_{n-1})\longleftrightarrow\bar{b}(x)=\overline{b_0+b_1x+\cdots+b_{n-1}x^{n-1}}$$

如果$\bar{a}(x)\bar{b}(x)=\bar{c}(x)$，其中$c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$，则定义$\boldsymbol{a}$与$\boldsymbol{b}$的乘积为

$$\boldsymbol{ab}=\boldsymbol{c}=(c_0,\ c_1,\ \cdots,\ c_{n-1})$$

这样一来，就保持了运算

$$\boldsymbol{a}+\boldsymbol{b}\longleftrightarrow\bar{a}(x)+\bar{b}(x)$$

$$\boldsymbol{ab}\longleftrightarrow\bar{a}(x)\cdot\bar{b}(x)$$

$$\lambda\boldsymbol{a}\longleftrightarrow\lambda\bar{a}(x),\quad\lambda\in GF(2)$$

因此，$GF(2)$上秩为n的交换代数$GF(2)/x^n-1$就与定义了向量乘法运算的n维向量空间建立了同构的关系。于是，V_n也构成了一个$GF(2)$上秩为n的交换代数。

有了这种观点以后，在编码理论中，我们就不只是把码字的集合视为V_n的一个线性子空间，而是把它视为代数V_n的一个**子代数**（即V_n的一个子集合，且按照V_n中的运算构成代数）。这就是我们所得到的线性码的一种同构表示。

下面介绍关于线性码的另一种更为简洁的同构表示。

命$F_n[x]$表示域F上次数低于n的全体多项式所成的集合。显然，$F_n[x]$构成F上的一个n维线性空间，它的基底是

$$1, \ x, \ x^2, \ \cdots, \ x^{n-1}$$

如果规定 $x^n=1$，则上述基底就构成一个 n 阶循环群，记为 $\langle x\rangle$。设

$$a(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$$
$$b(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}$$

是 $F_n[x]$ 中的两个多项式，在乘积 $a(x)b(x)$ 中按照 $x^n=1$ 消去高于 $n-1$ 的项，就得到

$$c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}\in F_n[x]$$

我们定义

$$c(x)=a(x)b(x)$$

不难验证，根据如此定义的乘法运算，$F_n[x]$ 构成一个域 F 上秩为 n 的交换代数，称为域 F 上 $\langle x\rangle$ 的群代数，记为 FG。

现在证明群代数 $F_n[x]$ 和 $F[x]/x^n-1$ 同构。可以如下建立同构对应关系：

$F_n[x]$		$F[x]/x^n-1$
$a(x)$	$\longleftrightarrow$	$\bar{a}(x)$
$a(x)+b(x)$	$\longleftrightarrow$	$\bar{a}(x)+\bar{b}(x)$
$a(x)b(x)$	$\longleftrightarrow$	$\bar{a}(x)\bar{b}(x)$
$\lambda a(x)$	$\longleftrightarrow$	$\lambda\bar{a}(x)$

类似地，群代数 FG 与 V_n 同构。事实上

$$a=(a_0, \ a_1, \ \cdots, \ a_{n-1})\longleftrightarrow a(x)=a_0+a_1x+\cdots+a_nx^{n-1}$$
$$a+b\longleftrightarrow a(x)+b(x)$$
$$ab\longleftrightarrow a(x)b(x)$$
$$\lambda a\longleftrightarrow\lambda a(x)$$

因此，我们也可以把码字的集合视为群代数 FG 的一个子群代数，这就得到了线性码的另一种同构表示。在编码理论中，常常交替地利用这两种同构表示。

例3.8.1　考虑 $GF(2)$ 上的 3 维向量空间 V_3（作为代数）的两种表示。一种是作为 $GF(2)[x]/x^3-1$，其运算见表 3-2

表 3-2

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$
$\overline{x^2}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\overline{x^2+1}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\overline{x^2+x}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x^2+x+1}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

表 3-3

·	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x^2}$	$\overline{x^2+x}$	$\bar{1}$	$\overline{x+1}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x+1}$	$\bar{0}$
$\overline{x^2}$	$\bar{0}$	$\overline{x^2}$	$\bar{1}$	$\overline{x^2+1}$	$\bar{x}$	$\overline{x^2+x}$	$\overline{x+1}$	$\overline{x^2+x+1}$
$\overline{x^2+1}$	$\bar{0}$	$\overline{x^2+1}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2+x}$	$\overline{x+1}$	$\overline{x^2+1}$	$\bar{0}$
$\overline{x^2+x}$	$\bar{0}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x+1}$	$\overline{x+1}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\bar{0}$
$\overline{x^2+x+1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x^2+x+1}$	$\bar{1}$	$\overline{x^2+x+1}$	$\bar{0}$	$\bar{0}$	$\overline{x^2+x+1}$

和表 3-3。

另一种是作为 $GF(2)$ 上 3 阶循环群 $\langle x\rangle$ 的群代数（$x^3=1$），其运算见表 3-2，表 3-3，只需把每一个多项式上边的横线去掉即可。例如，群代数中两个多项式 x^2+x+1 与 x^2+1 的乘积为

$$
\begin{aligned}
(x^2+x+1)(x^2+1) &= x^4+x^3+x^2+x^2+x+1 \\
&= x+1+x+1=0
\end{aligned}
$$

在群代数中的乘法运算显然比多项式剩余类代数中相应的乘法运算要简单得多。

第四章　循环空间与循环码

§4.1　线性变换的概念

大家知道，线性函数

$$y=f(x)=ax$$

有如下的线性性质：

$$f(x_1+x_2)=f(x_1)+f(x_2),\quad f(\lambda x)=\lambda f(x) \qquad (4\text{-}1)$$

除数以外，其它对象之间的变换也常常具有类似于式（4-1）的性质，这就导致了所谓"线性变换"的概念。我们先从"变换"的概念谈起。

定义4.1.1　设V和W是域F上的线性空间。若对于V中任意向量$\boldsymbol{x}$，按照一定的规律T，都有W中唯一确定的向量$\boldsymbol{y}$与之对应，则称T为空间V到空间W的一个变换，记为$\boldsymbol{y}=T(\boldsymbol{x})$，或$T:V\to W$。

今后所说的线性空间，均指在一个域F上的线性空间。

定义4.1.2　如果线性空间V到W的变换T具有下述（线性）性质：

（1）对于任何$\boldsymbol{x}_1$，$\boldsymbol{x}_2\in V$，恒有

$$T(\boldsymbol{x}_1+\boldsymbol{x}_2)=T(\boldsymbol{x}_1)+T(\boldsymbol{x}_2)$$

（2）对于任何$\lambda\in F$及任何$x\in V$，恒有

$$T(\lambda \boldsymbol{x})=\lambda T(\boldsymbol{x})$$

则称T为V到W的一个线性变换。

例4.1.1　考虑域F上的n维向量空间V_n到V_n的线性变换T：

$$\left.\begin{aligned}
y_1&=a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n\\
y_2&=a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n\\
&\cdots\\
y_n&=a_{n1}x_1+a_{n2}x_2+\cdots+a_{nn}x_n
\end{aligned}\right\} \qquad (4\text{-}2)$$

其中 $a_{ij}\in F$。按照变换 T，任意 $\boldsymbol{x}=(x_1, x_2, \cdots, x_n)\in V_n$ 根据式（4-2）被变为 $\boldsymbol{y}=(y_1, y_2, \cdots, y_n)\in V_n$，即

$$T(\boldsymbol{x})=\boldsymbol{y}$$

我们可以用矩阵方法将式（4-2）简写为下述形式：

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}=\begin{pmatrix} a_{11} & a_{12}\cdots a_{1n} \\ a_{21} & a_{22}\cdots a_{2n} \\ & \cdots \\ a_{n1} & a_{n2}\cdots a_{nn} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

其中

$$A=\begin{pmatrix} a_{11} & a_{12}\cdots a_{1n} \\ a_{21} & a_{22}\cdots a_{2n} \\ & \cdots \\ a_{n1} & a_{n2}\cdots a_{nn} \end{pmatrix}$$

为变换式（4-2）的系数矩阵。

变换 T 还可以写成更简单的形式

$$[y_1, y_2, \cdots, y_n]=[x_1, x_2, \cdots, x_n]A'$$

其中 A' 是矩阵 A 的转置矩阵。

现在证明 T 是线性变换。设

$$\boldsymbol{x}_1=(\xi_1, \xi_2, \cdots, \xi_n),\quad \boldsymbol{x}_2=(\eta_1, \eta_2, \cdots, \eta_n)$$

则

$$\begin{aligned} T(\boldsymbol{x}_1+\boldsymbol{x}_2) &= [\xi_1+\eta_1, \xi_2+\eta_2, \cdots, \xi_n+\eta_n]A' \\ &= [\xi_1, \xi_2, \cdots, \xi_n]A'+[\eta_1, \eta_2, \cdots, \eta_n]A' \\ &= T(\boldsymbol{x}_1)+T(\boldsymbol{x}_2) \end{aligned}$$

$$\begin{aligned} T(\lambda\boldsymbol{x}_1) &= [\lambda\xi_1, \lambda\xi_2, \cdots, \lambda\xi_n]A' \\ &= \lambda([\xi_1, \xi_2, \cdots, \xi_n]A') \\ &= \lambda T(\boldsymbol{x}_1) \end{aligned}$$

下面我们讨论线性变换与矩阵之间的联系。

定理4.1.1 设 V_n 是域 F 上的 n 维线性空间，$\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_n$ 是它的一组基底，且 $\boldsymbol{g}_1, \boldsymbol{g}_2, \cdots, \boldsymbol{g}_n$ 是 V_n 的任意一组向量。于是当且仅当一个 V_n 到其自身的线性变换 T，使得

$$T(\boldsymbol{e}_1)=\boldsymbol{g}_1,\ T(\boldsymbol{e}_2)=\boldsymbol{g}_2,\ \cdots,\ T(\boldsymbol{e}_n)=\boldsymbol{g}_n \qquad (4\text{-}3)$$

并且这一变换由

$$T(\xi_1 e_1+\xi_2 e_2+\cdots+\xi_n e_n)=\xi_1 g_1+\xi_2 g_2+\cdots+\xi_n g_n$$

定义。

证明 对于任意 $x\in V_n$，x 可按基底表成

$$x=\xi_1 e_1+\xi_2 e_2+\cdots+\xi_n e_n$$

定义

$$T(x)=\xi_1 g_1+\xi_2 g_2+\cdots+\xi_n g_n$$

现在证明 T 是线性变换。事实上，

$$\begin{aligned}T(\lambda x)&=T(\lambda\xi_1 e_1+\lambda\xi_2 e_2+\cdots+\lambda\xi_n e_n)\\&=\lambda\xi_1 T(e_1)+\lambda\xi_2 T(e_2)+\cdots+\lambda\xi_n T(e_n)\end{aligned}$$

变换 T 显然满足

$$T(e_1)=g_1,\ T(e_2)=g_2,\ \cdots,\ T(e_n)=g_n$$

因此

$$\begin{aligned}T(\lambda x)&=\lambda\xi_1 g_1+\lambda\xi_2 g_2+\cdots+\lambda\xi_n g_n\\&=\lambda(\xi_1 g_1+\xi_2 g_2+\cdots+\xi_n g_n)=\lambda T(x)\end{aligned}$$

其次令 $y=\eta_1 e_1+\eta_2 e_2+\cdots+\eta_n e_n\in V_n$

则有

$$\begin{aligned}T(x+y)&=T((\xi_1+\eta_1)e_1+\cdots+(\xi_n+\eta_n)e_n)\\&=(\xi_1 g_1+\cdots+\xi_n g_n)+(\eta_1 g_1+\cdots+\eta_n g_n)\\&=T(x)+T(y)\end{aligned}$$

最后我们证明满足式（4-3）的线性变换是唯一的。假如另有一个 V_n 到其自身的线性变换 T_1，也满足

$$T_1(e_1)=g_1,\ T_1(e_2)=g_2,\ \cdots,\ T_1(e_n)=g_n$$

则对任意 $x=\xi_1 e_1+\xi_2 e_2+\cdots+\xi_n e_n\in V_n$ 恒有

$$\begin{aligned}T_1(x)&=T_1(\xi_1 e_1+\xi_2 e_2+\cdots+\xi_n e_n)\\&=\xi_1 T(e_1)+\xi_2 T(e_2)+\cdots+\xi_n T(e_n)\\&=\xi_1 g_1+\xi_2 g_2+\cdots+\xi_n g_n\\&=T(x)\end{aligned}$$

因此，$T=T_1$。（证毕）

这一定理说明，在取定 V_n 的基底 e_1，e_2，$\cdots$，e_n 之后，V_n 到 V_n 的线性变换 T 由 n 个向量 g_1，g_2，$\cdots$，g_n 完全决定。设

$(a_{i1}, a_{i2}, \cdots, a_{in})$ 是 g_i 在基底 $e_1, e_2, \cdots, e_n$ 下的坐标，即

$$\left.\begin{aligned} T(e_1) &= g_1 = a_{11}e_1 + a_{12}e_2 + \cdots + a_{1n}e_n \\ T(e_2) &= g_2 = a_{21}e_1 + a_{22}e_2 + \cdots + a_{2n}e_n \\ &\cdots\cdots \\ T(e_n) &= g_n = a_{n1}e_1 + a_{n2}e_2 + \cdots + a_{nn}e_n \end{aligned}\right\} \tag{4-4}$$

因此，线性变换 T 由矩阵

$$A = \begin{pmatrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} & a_{22} \cdots a_{2n} \\ & \cdots \\ a_{n1} & a_{n2} \cdots a_{nn} \end{pmatrix}$$

完全决定。于是**在取定基底之后，V_n 到 V_n 的线性变换 T 与 n 阶方阵之间具有一一对应的关系**。事实上，给定 T 后，对于取定的基底可得 n 个向量 $g_1 = T(e_1), \cdots, g_n = T(e_n)$，从而就有 a_{ij}，即得到矩阵 A。反之给定 A 后，可按式 (4-4) 求出 $g_1, \cdots, g_n$，从而由定理 4.1.1 得到线性变换 T。

称矩阵 A 为**线性变换 T 在基底 $e_1, e_2, \cdots, e_n$ 之下的矩阵**。

再看例 4.1.1，若取基底

$e_1 = (1, 0, 0, \cdots, 0)$，$e_2 = (0, 1, 0, \cdots, 0), \cdots,$

$e_n = (0, 0, 0, \cdots, 1)$，

则有

$$\begin{aligned} g_1 = T(e_1) &= (a_{11}, a_{21}, \cdots, a_{n1}) \\ &= a_{11}e_1 + a_{21}e_2 + \cdots + a_{n1}e_n \\ g_2 = T(e_2) &= (a_{12}, a_{22}, \cdots, a_{n2}) \\ &= a_{12}e_1 + a_{22}e_2 + \cdots + a_{n2}e_n \\ &\cdots \\ g_n = T(e_n) &= (a_{1n}, a_{2n}, \cdots, a_{nn}) \\ &= a_{1n}e_1 + a_{2n}e_2 + \cdots + a_{nn}e_n \end{aligned}$$

因此式 (4-2) 所决定的变换 T 的矩阵为

$$\begin{pmatrix} a_{11} & a_{21} \cdots a_{n1} \\ a_{12} & a_{22} \cdots a_{n2} \\ \vdots & \vdots \quad\ \ \vdots \\ a_{1n} & a_{2n} \cdots a_{nn} \end{pmatrix}$$

它是式（4-2）的系数矩阵的转置矩阵。

§4.2 线性变换的代数

这一节，我们讨论V_n到V_n的线性变换的运算与矩阵运算之间的联系。

设V_n是域F上的n维线性空间，e_1，e_2，…，e_n是它的一组基底。在以下的讨论中，我们恒将这组基底固定。令T_A表示V_n到V_n的线性变换，且T_A在上述基底之下的矩阵为A。在§4.1中反映线性变换与其对应矩阵之间联系的式（4-4）可简写成下述形式

$$\begin{bmatrix} T_A(e_1) \\ T_A(e_2) \\ \vdots \\ T_A(e_n) \end{bmatrix} = \begin{pmatrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} a_{22} & \cdots a_{2n} \\ & \cdots \\ a_{n1} & a_{n2} \cdots a_{nn} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = A \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}$$

设T_A，T_B是两个线性变换，则由

$$T(x) = T_A(x) + T_B(x) \quad (x \in V_n)$$

所定义的变换T称为变换T_A与变换T_B之和，并记为$T = T_A + T_B$。不难看出，两个线性变换之和仍为线性变换。事实上

$$\begin{aligned} T(x_1 + x_2) &= T_A(x_1 + x_2) + T_B(x_1 + x_2) \\ &= (T_A(x_1) + T_B(x_1)) + (T_A(x_2) \\ &\quad + T_B(x_2)) \\ &= T(x_1) + T(x_2) \end{aligned}$$

同理可证

$$T(\lambda x) = \lambda T(x) \quad (\lambda \in F)$$

现在我们求两个线性变换之和$T = T_A + T_B$所对应的矩阵。由于

$$\begin{pmatrix} T_A(e_1) \\ T_A(e_2) \\ \vdots \\ T_A(e_n) \end{pmatrix} = A \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}, \quad \begin{pmatrix} T_B(e_1) \\ T_B(e_2) \\ \vdots \\ T_B(e_n) \end{pmatrix} = B \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}$$

故

$$\begin{pmatrix} T(e_1) \\ T(e_2) \\ \vdots \\ T(e_n) \end{pmatrix} = \begin{pmatrix} T_A(e_1)+T_B(e_1) \\ T_A(e_2)+T_B(e_2) \\ \vdots \\ T_A(e_n)+T_B(e_n) \end{pmatrix} = \begin{pmatrix} T_A(e_1) \\ T_A(e_2) \\ \vdots \\ T_A(e_n) \end{pmatrix} + \begin{pmatrix} T_B(e_1) \\ T_B(e_2) \\ \vdots \\ T_B(e_n) \end{pmatrix}$$

$$= A\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} + B\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = (A+B)\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}$$

这表明 $T=T_A+T_B$ 所对应的矩阵为 $A+B$。

由此我们得到一个重要结论：线性变换之和所对应的矩阵等于线性变换所对应的矩阵之和，即

$$T_A+T_B=T_{A+B} \tag{4-5}$$

设 $\alpha\in F$，T_A 是一个线性变换，则由

$$T(x)=\alpha T_A(x)$$

所定义的变换 T 称为 α 与变换 T_A 的乘积，记为 $T=\alpha T_A$。不难证明，αT_A 也是线性变换。由于

$$\begin{pmatrix} (\alpha T_A)(e_1) \\ (\alpha T_A)(e_2) \\ \vdots \\ (\alpha T_A)(e_n) \end{pmatrix} = \begin{pmatrix} \alpha(T_A(e_1)) \\ \alpha(T_A(e_2)) \\ \vdots \\ \alpha(T_A(e_n)) \end{pmatrix} = \alpha\begin{pmatrix} T_A(e_1) \\ T_A(e_2) \\ \vdots \\ T_A(e_n) \end{pmatrix}$$

$$= \alpha\left(A\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}\right) = (\alpha A)\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}$$

这表明 αT_A 所对应的矩阵为 αA。因此

$$T_{\alpha A}=\alpha T_A \tag{4-6}$$

对于线性变换 T_A 与 T_B，由等式

$$T(x)=T_B(T_A(x))$$

所定义的变换 T 称为变换 T_A 与 T_B 之乘积，记为 $T=T_AT_B$

我们证明，T_AT_B 仍为线性变换。事实上

$$\begin{aligned} T_AT_B(\boldsymbol{x}_1+\boldsymbol{x}_2)&=T_B(T_A(\boldsymbol{x}_1+\boldsymbol{x}_2))\\ &=T_B(T_A(\boldsymbol{x}_1)+T_A(\boldsymbol{x}_2))\\ &=T_B(T_A(\boldsymbol{x}_1))+T_B(T_A(\boldsymbol{x}_2))\\ &=T_AT_B(\boldsymbol{x}_1)+T_AT_B(\boldsymbol{x}_2)\end{aligned}$$

同理可证

$$T_AT_B(\lambda\boldsymbol{x})=\lambda T_AT_B(\boldsymbol{x})$$

现在求 T_AT_B 的矩阵。由于

$$\begin{pmatrix}(T_AT_B)(\boldsymbol{e}_1)\\(T_AT_B)(\boldsymbol{e}_2)\\ \vdots\\(T_AT_B)(\boldsymbol{e}_n)\end{pmatrix}=\begin{pmatrix}T_B(T_A(\boldsymbol{e}_1))\\T_B(T_A(\boldsymbol{e}_2))\\ \vdots\\T_B(T_A(\boldsymbol{e}_n))\end{pmatrix}$$

$$=\begin{pmatrix}T_B(a_{11}\boldsymbol{e}_1+a_{12}\boldsymbol{e}_2+\cdots+a_{1n}\boldsymbol{e}_n)\\T_B(a_{21}\boldsymbol{e}_1+a_{22}\boldsymbol{e}_2+\cdots+a_{2n}\boldsymbol{e}_n)\\ \cdots\\T_B(a_{n1}\boldsymbol{e}_1+a_{n2}\boldsymbol{e}_2+\cdots+a_{nn}\boldsymbol{e}_n)\end{pmatrix}$$

$$=\begin{pmatrix}a_{11}T_B(\boldsymbol{e}_1)+\cdots+a_{1n}T_B(\boldsymbol{e}_n)\\ \vdots\qquad\qquad\vdots\\a_{n1}T_B(\boldsymbol{e}_1)+\cdots+a_{nn}T_B(\boldsymbol{e}_n)\end{pmatrix}$$

$$=A\begin{pmatrix}T_B(\boldsymbol{e}_1)\\ \vdots\\T_B(\boldsymbol{e}_n)\end{pmatrix}=A\left(B\begin{pmatrix}\boldsymbol{e}_1\\ \vdots\\ \boldsymbol{e}_n\end{pmatrix}\right)=(AB)\begin{pmatrix}\boldsymbol{e}_1\\ \vdots\\ \boldsymbol{e}_n\end{pmatrix}$$

这表明 T_AT_B 所对应的矩阵为 AB，因此

$$T_{AB}=T_AT_B \tag{4-7}$$

最后我们考虑域 F 上全部 n 阶矩阵所成之集合。由例 2.1.4，这一集合构成 n^2 维线性空间。此外，由于矩阵运算满足乘法结合律、分配律，因而这一集合还构成环，并且满足

$$\lambda(AB)=(\lambda A)B=A(\lambda B),\ (\lambda\in F)$$

这样一来，域 F 上全体 n 阶矩阵的集合就构成一个秩为 n^2 的代数，称之为 n 阶矩阵代数。

再看 V_n 到 V_n 的全体线性变换的集合。由于线性变换与 n 阶矩阵之间的一一对应关系

$$A \longleftrightarrow T_A$$

并且根据式（4-5）、（4-6）和（4-7）

$$A+B \longleftrightarrow T_A+T_B$$

$$\alpha A \longleftrightarrow \alpha T_A$$

$$AB \longleftrightarrow T_A T_B$$

因此全体线性变换的集合与 n 阶矩阵代数同构。于是 V_n 到 V_n 的全体线性变换的集合也构成一个秩为 n^2 的代数。不过由于矩阵乘法不满足交换律，故这两个代数都不是交换代数。

综上所述，我们有

定理4.2.1 域 F 上的 n 维线性空间 V_n 到其自身的全体线性变换所成的集合构成一个与域 F 上 n 阶矩阵代数同构的代数，其秩为 n^2。

由此看来矩阵的理论与线性变换的理论是平行的。

§4.3 最小多项式、伴侣矩阵

根据前一节的结果，我们可以建立矩阵多项式和变换多项式的概念。

设 T 为域 F 上 n 维线性空间 V_n 到 V_n 的线性变换，我们可以定义变换 T 的各次幂

$$T^2=TT,\ T^3=TT^2,\ \cdots$$

并且规定

$$T^0=I$$

此处 I 是单位变换，即

$I(\boldsymbol{x})=\boldsymbol{x}$，对一切 $\boldsymbol{x}\in V_n$

对于域 F 上任意多项式

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_kx^k$$

我们相应地得到一个变换多项式

$$f(T)=a_0I+a_1T+a_2T^2+\cdots+a_kT^k$$

和一个矩阵多项式

$$f(A)=a_0I+a_1A+a_2A^2+\cdots+a_kA^k$$

其中A是变换T的矩阵，I是$n\times n$单位方阵。

由于n阶矩阵代数的秩为n^2，故n^2+1个矩阵

I，A，A^2，…，A^{n^2}

一定线性相关，即存在不全为零的$a_i\in F$（$i=0$，1，2，…，n^2），使得

$$f(A)=a_0I+a_1A+a_2A^2+\cdots+a_{n^2}A^{n^2}=0$$

根据变换与矩阵的同构关系，自然有

$$f(T)=a_0I+a_1T+a_2T^2+\cdots+a_{n^2}T^{n^2}=0$$

注意，等式右边的0代表零变换，即

$0(x)=0$，对一切$x\in V_n$

这样看来，对于任何线性变换T，总有一个非零多项式$f(x)$存在，使

$$f(T)=0$$

定理4.3.1 对于域F上的V_n到V_n的任何线性变换T，恒存在唯一的F上的首一多项式$m(x)$，具有下述性质：

（1）$m(T)=0$；

（2）对于任意$f(x)\in F[x]$，若$f(T)=0$，则$m(x)\mid f(x)$。

证明 考虑下述集合

$$M\triangleq\{f(x)\mid f(x)\in F[x],\ f(T)=0\}$$

它显然构成多项式环$F[x]$的理想。由定理3.7.4，M是$F[x]$的主理想。于是，存在唯一的首一多项式$m(x)$，使得$M=\langle m(x)\rangle$。因此，对任意$f(x)\in F[x]$，$f(T)=0$，必有$m(x)\mid f(x)$。 （证毕）

称具有定理4.3.1中的性质（1）和（2）的$m(x)$为**线性变换T的最小多项式**。

显然，线性变换T的最小多项式就是$F[x]$中满足$f(T)=0$的次数最低的首一多项式。

由于矩阵与线性变换的同构关系，自然可以定义n阶矩阵的最小多项式。

域F上任意n次首一多项式

$$g(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+x^n$$

都对应一个$n\times n$矩阵

$$C_g=\begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & -c_3 & & -c_{n-1} \end{pmatrix}=\begin{pmatrix} 0 & \\ 0 & \\ 0 & I_{n-1} \\ \vdots & \\ 0 & \\ -c_0\cdots\cdots & -c_{n-1} \end{pmatrix}$$

其中I_{n-1}为$n-1$阶单位矩阵。

称C_g为首一多项式$g(x)$的伴侣矩阵。

定理4.3.2 设$g(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+x^n$是域$F$上的任意首一多项式，则它的伴侣矩阵$C_g$恰以$g(x)$为最小多项式。

证明 设T为以C_g为矩阵的线性变换$(V_n\to V_n)$，且设

e_1，e_2，$\cdots$，e_n

为V_n的一组基底，则

$$T(e_1)=e_2$$
$$T(e_2)=T(T(e_1))=T^2(e_1)=e_3$$
$$T(e_3)=T(T^2(e_1))=T^3(e_1)=e_4$$
$$\cdots$$
$$T(e_{n-1})=T(T^{n-2}(e_1))=T^{n-1}(e_1)=e_n$$
$$T(e_n)=T(T^{n-1}(e_1))=T^n(e_1)=-c_0e_1-c_1e_2$$
$$-\cdots-c_{n-1}e_n=-c_0e_1-c_1T(e_1)-\cdots$$
$$-c_{n-1}T^{n-1}(e_1)=(-c_0I-c_1T-\cdots-c_{n-1}T^{n-1})(e_1)$$

因此

$$(c_0I+c_1T+\cdots+c_{n-1}T^{n-1}+T^n)(e_1)=0$$

亦即

$$g(T)(e_1)=0$$

由于

$$e_1,\ e_2=T(e_1),\ \cdots,\ e_n=T^{n-1}(e_1)$$

是V_n的基底，故任意$x\in V_n$恒可表为

$$
\begin{aligned}
x &= a_0e_1 + a_1e_2 + \cdots + a_{n-1}e_n \\
&= a_0e_1 + a_1T(e_1) + \cdots + a_{n-1}T^{n-1}(e_1) \\
&= (a_0I + a_1T + \cdots + a_{n-1}T^{n-1})(e_1) \\
&= f(T)(e_1) \qquad (4\text{-}8)
\end{aligned}
$$

其中

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$$

是域F上次数$\leqslant n-1$的多项式。因此，对于任意$x\in V_n$，恒有

$$
\begin{aligned}
g(T)(x) &= g(T)(f(T)(e_1)) \\
&= f(T)(g(T)(e_1)) = 0
\end{aligned}
$$

于是

$$g(T) = 0$$

即$g(T)$是零变换。

现在证明n次多项式$g(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + x^n$是满足条件$g(T)=0$的次数最低的多项式。设

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \quad (a_i\text{不全为}0)$$

是任意次数$<n$的多项式。由于a_i不全为0，故V_n中的元素

$$x = a_0e_1 + a_1e_2 + \cdots + a_{n-1}e_n \neq 0$$

由式（4-8）

$$f(T)(e_1) = x \neq 0$$

这表明$f(T)\neq 0$。因此，$g(x)$是变换T的最小多项式，从而$g(x)$为C_g的最小多项式。 〈证毕〉

§4.4 循环空间

在编码理论中所说的循环码，实际上是一个循环空间。在讨论循环空间之前，我们还需要不变子空间的概念。

定义4.4.1 设V_n是域F上的n维线性空间，T是V_n到V_n的线性变换。如果V_n的线性子空间S满足下述条件：

对任意$x\in S$，恒有$T(x)\in S$；

则称S为变换T的不变子空间。

如果S是T的不变子空间，我们就可以把变换T视为子空间S到S的线性变换。这时我们说变换

$$T: S \to S$$

为由原变换

$$T: V_n \to V_n$$

诱导出来的线性变换。

下面我们介绍一种生成不变子空间的方法。

设T是V_n到V_n的线性变换，$\alpha \in V_n$。显然，T的任意包含α的不变子空间必然包含所有形如$f(T)(\alpha)$的元素，其中$f(T)$是变换T的任意多项式。考虑集合

$$Z_\alpha \triangleq \{ f(T)(\alpha) | f(x) \in F[x] \}$$

不难证明Z_α是V_n的线性子空间，并且是T的不变子空间。因此，Z_α是T的所有包含α的不变子空间中的最小者。

称Z_α为**由元素α生成的T一循环子空间**。

现在我们来看一看，循环子空间的循环特性表现在什么地方。

当$\alpha = \mathbf{0}$时，$Z_\alpha = \{\mathbf{0}\}$，我们对这一子空间不感兴趣。

设$g(x) = c_0 + c_1 x + \cdots + c_{d-1} x^{d-1} + x^d$

为诱导变换

$$T: Z_\alpha \to Z_\alpha$$

的最小多项式，且设$\alpha \neq \mathbf{0}$，则Z_α中的向量组

$$\alpha, \quad T(\alpha), \quad \cdots, \quad T^{d-1}(\alpha) \tag{4-9}$$

是线性独立的。否则，若存在F中不全为零的$a_0, a_1, \cdots, a_{d-1}$，使得

$$a_0\alpha + a_1 T(\alpha) + \cdots + a_{d-1} T^{d-1}(\alpha) = (a_0 I + a_1 T + \cdots + a_{d-1} T^{d-1})(\alpha)$$
$$= \phi(T)(\alpha) = \mathbf{0}$$

其中

$$\phi(x) = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1}$$

则对于任意$\boldsymbol{x} = f(T)(\alpha) \in Z_\alpha$，恒有

$$\phi(T)(\boldsymbol{x}) = \phi(T)(f(T)(\alpha)) = f(T)(\phi(T)(\alpha)) = \mathbf{0}$$

这表明$\phi(T) = 0$。这与$g(x)$是诱导变换T的最小多项式的假定矛盾。因此向量组（4-9）是线性独立的。同时式（4-9）

还构成子空间 Z_α 的基底。由于

$$g(T)(\alpha)=c_0\alpha+c_1T(\alpha)+\cdots+c_{d-1}T^{d-1}(\alpha)+T^d(\alpha)=0$$

因此，

$$T^d(\alpha)=-c_0\alpha-c_1T(\alpha)-\cdots-c_{d-1}T^{d-1}(\alpha) \qquad (4\text{-}10)$$

这样一来，Z_α 中的任意向量 $f(T)(\alpha)$ 皆可表为向量组（4-9）的线性组合。因为 $f(T)(\alpha)$ 中如有高于 $d-1$ 次的项

$$T^d(\alpha),\ T^{d+1}(\alpha),\ \cdots$$

则可按式（4-10）化为式（4-9）的线性组合。

称式（4-9）为循环子空间 Z_α 的**循环基底**。

反过来，如果线性空间 V_n 的子空间 S 以

$$\alpha,\ T(\alpha),\ \cdots,\ T^{d-1}(\alpha)$$

为基底，则 S 必为由 α 生成的 T—循环子空间。任意 $x\in S$ 都是 α，$T(\alpha)$，$\cdots$，$T^{d-1}(\alpha)$ 的线性组合，即为某个 $f(T)(\alpha)$。反之，任意 $f(T)(\alpha)$ 亦必为 α，$T(\alpha)$，$\cdots$，$T^{d-1}(\alpha)$ 的线性组合，因为 $f(T)(\alpha)$ 中高于 $d-1$ 次的项可按式（4-10）化为式（4-9）的线性组合。因此

$$S=Z_\alpha=\{f(T)(\alpha)\mid f(x)\in F[x]\}$$

当 $T^d(\alpha)$ 按式（4-10）表成基底的线性组合时，多项式

$$g(x)=c_0+c_1x+\cdots+c_{d-1}x^{d-1}+x^d$$

显然必为诱导变换 $T(Z_\alpha\to Z_\alpha)$ 的最小多项式。

综上所述，我们得到

定理 4.4.1 设 S 为域 F 上 n 维线性空间 V_n 的子空间，T 为 V_n 到 V_n 的线性变换。于是 S 为 T—循环子空间，当且仅当存在 $\alpha\neq 0\in S$，使得

$$\alpha,\ T(\alpha),\ \cdots,\ T^{d-1}(\alpha)$$

构成 S 的基底。并且，此时循环子空间 S 的维数等于诱导变换 $T(S\to S)$ 的最小多项式

$$g(x)=c_0+c_1x+\cdots+c_{d-1}x^{d-1}+x^d$$

的次数 d，而 $g(x)$ 又与 $T^d(\alpha)$ 通过基底的表达式

$$T^d(\alpha)=-c_0\alpha-c_1T(\alpha)-\cdots-c_{d-1}T^{d-1}(\alpha)$$

互相联系。

最后我们讨论 T—循环子空间的诱导变换的矩阵。

设 Z_α 为 V_n 的 d 维 T—循环子空间，则

$$\alpha, \ T(\alpha), \ \cdots, \ T^{d-1}(\alpha)$$

为 Z_α 的基底。令 $T^d(\alpha)$ 通过基底的表达式为式（4-10），则有

$$T(\alpha)=T(\alpha)$$
$$T(T(\alpha))=T^2(\alpha)$$
$$\cdots$$
$$T(T^{d-2}(\alpha))=T^{d-1}(\alpha)$$
$$T(T^{d-1}(\alpha))=T^d(\alpha)=-c_0\alpha-c_1T(\alpha)-\cdots-c_{d-1}T^{d-1}(\alpha)$$

因此诱导变换

$$T:Z_\alpha \to Z_\alpha$$

在基底 α，$T(\alpha)$，…，$T^{d-1}(\alpha)$ 之下的矩阵为

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{d-1} \end{pmatrix}$$

它正是诱导变换 $T(Z_\alpha \to Z_\alpha)$ 的最小多项式 $g(x)=c_0+c_1x+\cdots+c_{d-1}x^{d-1}+x^d$ 的伴侣矩阵。

因此，我们有

定理 4.4.2 设 Z_α 为 V_n 的 d 维 T—循环子空间，则诱导变换

$$T:Z_\alpha \to Z_\alpha$$

在基底

$$\alpha, \ T(\alpha), \ \cdots, \ T^{d-1}(\alpha)$$

之下的矩阵恰为 T 的最小多项式的伴侣矩阵。

§4.5 循环码、系统循环码

这一节我们讨论有限域 $GF(q)$ 上的循环码。设 V_n 是 $GF(q)$ 上的 n 维向量空间，由 §3.8，V_n 与剩余类代数 $GF(q)$

$[x]\bmod(x^n-1)$ 同构，同时也与 $GF(q)$ 上 $\langle x\rangle$ 的群代数 FG 同构。以下我们将根据需要，用 V_n 的这两种同构来表示 V_n 中的向量。以下我们总假定 $(n, q)=1$。

定义 4.5.1 V_n 的 k 维子空间 V_k 称为一个**循环码**，如果对于任意 $(a_0, a_1, \cdots, a_{n-1})\in V_n$，只要 $(a_0, a_1, \cdots, a_{n-1})\in V_k$，就必然有 $(a_{n-1}, a_0, a_1, \cdots, a_{n-2})\in V_k$。

下面的定理给出循环码的一个重要标志。

定理 4.5.1 V_k 是循环码当且仅当 V_k 是群代数 FG 中的理想。

证明 设 V_k 是理想，且 $(a_0, a_1, \cdots, a_{n-1})\in V_k$，即 $a_0+a_1x+\cdots+a_{n-1}x^{n-1}\in V_k$。于是，$a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ 的倍式 $x(a_0+a_1x+\cdots+a_{n-1}x^{n-1})$ 也是 V_k 中的元素。注意到 $x^n=1$，则有

$$x(a_0+a_1x+\cdots+a_{n-1}x^{n-1})=a_{n-1}+a_0x+\cdots+a_{n-2}x^{n-1}\in V_k$$

亦即

$$(a_{n-1}, a_0, \cdots, a_{n-2})\in V_k。$$

因此，V_k 是循环码。

反之，设 V_k 是循环码。对于 $a(x)$，$b(x)\in V_k$，因 V_k 是线性子空间，故 $a(x)-b(x)\in V_k$。此外若 $a(x)\in V_k$，则 $xa(x)\in V_k$。进一步，$x^2a(x)$，$x^3a(x)$，$\cdots$ 也属于 V_k。因此对于任意多项式 $p(x)\in FG$，都有 $p(x)a(x)\in V_k$。这表明 V_k 是 FG 中的理想。〈证毕〉

由于 FG 与 $GF(q)\bmod(x^n-1)$ 同构，因此 V_k 是 $GF(q)\bmod(x^n-1)$ 的理想。根据定理 3.7.5，V_k 是 $GF(q)\bmod(x^n-1)$ 的主理想。若设 $g(x)$ 为该主理想的生成多项式，则 $g(x)|(x^n-1)$，并且 V_k 中的全体码多项式的集合由 $g(x)$ 的一切可能的倍式组成。反之对于任意 $g(x)$，只要 $g(x)|(x^n-1)$，则由 $g(x)$ 的一切倍式所组成的集合就构成 FG 的一个主理想，从而构成一个循环码。

称 $g(x)$ 为循环码的生成多项式。

下面，我们讨论循环码的生成矩阵与一致校验矩阵。

设 $g(x)$ 为 (n, k) 循环码 V_k 的生成多项式，且设

$$x^n - 1 = g(x)h(x)$$

我们证明

$$\deg g(x) = n - k, \quad \deg h(x) = k$$

设

$$g(x) = g_0 + g_1 x + \cdots + g_r x^r, \quad (g_r \neq 0)$$

则 $a(x) \in V_k$ 可表为

$$a(x) = (m_0 + m_1 x + \cdots + m_{n-r-1} x^{n-r-1}) g(x)$$

这样的码多项式共计有 2^{n-r} 个。但是，V_k 中的码向量共有 2^k个。因此 $k = n - r$，即 $r = n - k$。这表明，$\deg g(x) = n - k$，从而，$\deg h(x) = k$。

进一步，码多项式组

$$g(x), \ xg(x), \ \cdots, \ x^{k-1} g(x) \tag{4-11}$$

在 V_k(作为 FG 中的理想) 中是线性独立的。

若

$$a_0 g(x) + a_1 x g(x) + \cdots + a_{k-1} x^{k-1} g(x) = a_0(g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}) + a_1 x(g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}) + \cdots + a_{k-1} x^{k-1}(g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}) = 0$$

则将上式合并成一个 x 的多项式后，其系数应当等于零。据此，首先常数项应当为零

$$a_0 g_0 = 0$$

但是 $g_0 \neq 0$。否则 $g(x) = g_1 x + \cdots + g_{n-k} x^{n-k}$ 以 $x = 0$ 为根，此与 $g(x) | (x^n - 1)$ 的假定矛盾。因此 $a_0 = 0$。紧接着应当有

$$a_1 g_0 = 0$$

从而 $a_1 = 0$，余此类推。最后得，

$$a_0 = a_1 = \cdots = a_{k-1} = 0$$

更进一步，我们证明式 (4-11) 构成 V_k 的基底。如前所述，该循环码 V_k 中的任意码多项式 $a(x)$ 皆可表为

$$a(x) = (m_0 + m_1 x + \cdots + m_{k-1} x^{k-1}) g(x)$$

$$=m_0g(x)+m_1xg(x)+\cdots+m_{k-1}x^{k-1}g(x)$$

注意到V_n(作为群代数FG) 以

$$1,\ x,\ x^2,\ \cdots,\ x^{n-1}$$

为基底。因此，循环码V_k作为线性分组码看待，它的生成矩阵是

$$G=\begin{pmatrix} g_0 & g_1 & g_2\cdots & g_{n-k} & 0 & \overbrace{0 & \cdots & 0}^{k-1\text{个}0} \\ 0 & g_0 & g_1\cdots & \vdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & g_0\cdots & & \vdots & g_{n-k} & \cdots & 0 \\ \vdots & \vdots & \vdots\cdots & & & \vdots & \cdots & \vdots \\ \underbrace{0 & 0 & 0\cdots 0}_{k-1\text{个}0} & g_0 & g_1 & \cdots & & g_{n-k} \end{pmatrix} \tag{4-12}$$

此为$k\times n$矩阵。

假设

$$h(x)=h_0+h_1x+\cdots+h_kx^k$$

注意到

$$g(x)h(x)=(g_0+g_1x+\cdots+g_{n-k}x^{n-k})(h_0+h_1x+\cdots+h_kx^k)=x^n-1$$

由此得

$$\left.\begin{aligned} & g_0h_0=-1 \\ & g_0h_1+g_1h_0=0 \\ & \cdots \\ & g_0h_i+g_1h_{i-1}+\cdots+g_{n-k}h_{i-(n-k)}=0 \\ & \cdots \\ & g_0h_{n-1}+g_1h_{n-2}+\cdots+g_{n-k}h_{k-1}=0 \\ & g_{n-k}h_k=1 \end{aligned}\right\} \tag{4-13}$$

或者，简写为

$$\left.\begin{aligned} & g_0h_i+g_1h_{i-1}+\cdots+g_{n-k}h_{i-(n-k)}=0 \\ & \qquad (i=1,\ 2,\ \cdots,\ n-1) \\ & g_0h_0+g_{n-k}h_k=0 \end{aligned}\right\}$$

因此，循环码V_k的一致校验矩阵为

$$H=\begin{pmatrix} h_k & h_{k-1} & & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & \vdots & h_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix} \tag{4-14}$$

由式（4-13）显然可得

$$GH'=\mathbf{0}$$

其中 $\mathbf{0}$ 是 $k\times(n-k)$ 零矩阵。

称 $h(x)$ 为循环码 V_k 的校验多项式。在循环码的研究中，通常以生成多项式代替生成矩阵，以校验多项式代替一致校验矩阵。并且循环码 V_k 的信息位个数（即空间 V_k 的维数 k）等于校验多项式 $h(x)$ 的次数，而其校验位（即多余数字）个数等于生成多项式 $g(x)$ 的次数。

其次我们讨论循环码与循环空间的联系。

视 V_n 为 FG 的同构，作变换

$$T(a(x))=xa(x),\quad a(x)\in V_n \tag{4-15}$$

显然 T 是 V_n 到 V_n 的线性变换。

前面已经看到，循环码 V_k 的基底为

$$g(x),\ xg(x),\ \cdots,\ x^{k-1}g(x)$$

亦即

$$g(x),\ T(g(x)),\ \cdots,\ T^{k-1}(g(x))$$

不妨设循环码 V_k 的校验多项式为首一多项式

$$h(x)=h_0+h_1x+\cdots+h_{k-1}x^{k-1}+x^k$$

于是

$$x^k=h(x)-h_0-h_1x-\cdots-h_{k-1}x^{k-1}$$

从而

$$x^kg(x)=h(x)g(x)-h_0g(x)-h_1xg(x)-\cdots-h_{k-1}x^{k-1}g(x)$$

注意到在 FG 中有 $h(x)g(x)=x^n-1=0$，因此

$$T^k(g(x))=-h_0g(x)-h_1T(g(x))-\cdots-h_{k-1}T^{k-1}(g(x))$$

由定理 4.4.1，循环码 V_k 为由 $g(x)$ 生成的 T—循环子空

间，其中$g(x)$是V_k的生成多项式，并且V_k的首一校验多项式$h(x)$恰为诱导变换

$$T: V_k \to V_k$$

最小多项式。

反之，若V_n的子空间V_k是由$g(x)$生成的T—循环子空间，其中T由式（4-15）定义，则V_k必为由$g(x)$生成的循环码。该循环子空间中的任意元素为

$$a_0 g(x) + a_1 T(g(x)) + \cdots + a_{k-1} T^{k-1}(g(x))$$
$$= (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) g(x)$$

即为$g(x)$的倍式。反过来，$g(x)$的任意倍式亦必为该循环子空间中的一个元素。因此V_k为由$g(x)$生成的理想，即V_k为由$g(x)$生成的循环码，从而$g(x) | (x^n - 1)$。

综上所述，我们有

定理 4.5.2 V_n的子空间V_k为由$g(x)$生成的循环码当且仅当V_k是由$g(x)$生成的T—循环子空间，其中T为由式（4-15）定义的V_n到V_n的线性变换。

例 4.5.1 设$n=7$，在$GF(2)$上，x^7-1可以分解成下列不可约因式

$$x^7 - 1 = (x-1)(x^3+x^2+1)(x^3+x+1)$$

关于$GF(q)$上x^n-1的因式分解问题，以后会讲到。这里读者不难验证上述因式分解的正确性。

取$g(x)=x^3+x+1$，我们就得到一个以

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

为生成矩阵的（7，4）循环码C。由于$h(x)=(x-1)(x^3+x^2+1)=x^4+x^2+x+1$，故$C$的一致校验矩阵为

$$H=\begin{pmatrix}1&0&1&1&1&0&0\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{pmatrix}$$

显然这个（7，4）循环码与二元汉明（7，4）码等价。事实上，只要将上述H矩阵施行列置换

$$\begin{pmatrix}1&2&3&4&5&6&7\\4&2&5&6&7&3&1\end{pmatrix}=(1\ 4\ 6\ 3\ 5\ 7)$$

就得到矩阵

$$\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix}$$

它正是（7，4）二元汉明码的一致校验矩阵（参看式（2-25））。

最后我们讨论如何将循环码化为系统循环码的问题。

设$g(x)$为（n，k）循环码V_k的生成多项式。由欧几里德除法

$$x^i=g(x)q_i(x)+r_i(x)$$

$$\deg r_i(x)<\deg g(x)=n-k，\text{或 } r_i(x)=0$$

$$i=n-k,\ n-k+1,\ \cdots,\ n-1$$

于是$x^i-r_i(x)=g(x)q_i(x)$是V_k中的码向量。不难看出k个向量

$$x^{n-k}-r_{n-k}(x),\ \cdots,\ x^{n-1}-r_{n-1}(x) \tag{4-16}$$

构成V_k的基底。若

$$a_{n-k}(x^{n-k}-r_{n-k}(x))+\cdots+a_{n-1}(x^{n-1}-r_{n-1}(x))$$
$$=g(x)(a_{n-k}q_{n-k}(x)+\cdots+a_{n-1}q_{n-1}(x))=0$$

则因

$$\deg q_{n-k}(x)=0,\ \cdots,\ \deg q_{n-1}(x)=k-1$$

故得

$$a_{n-k}=0,\ \cdots,\ a_{n-1}=0$$

若设

$$r_{n-k+l}(x)=r_{l0}+r_{l1}x+\cdots+r_{l,n-k-1}x^{n-k-1}$$

则循环码 V_k 在基底式（4-16）之下的矩阵为

$$G=\begin{pmatrix} -r_{n-k}(x)+x^{n-k} \\ -r_{n-k+1}(x)+x^{n-k+1} \\ \cdots \\ -r_{n-1}(x)+x^{n-1} \end{pmatrix}$$

$$=\begin{pmatrix} -r_{00} & -r_{01} & \cdots -r_{0\ n-k-1} & 1 & 0\cdots 0 \\ -r_{10} & -r_{11} & \cdots -r_{1\ n-k-1} & 0 & 1\cdots 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots\cdots\vdots \\ -r_{k-10} & -r_{k-11} & \cdots -r_{k-1\ n-k-1} & 0 & 0\cdots 1 \end{pmatrix}$$

$$=[R,\ I] \tag{4-17}$$

其中 R 为 $k\times(n-k)$ 矩阵，I 为 $k\times k$ 单位矩阵。

利用列的置换，也可以把式（4-17）变成

$$[I,\ R]$$

的形式。按照循环码的习惯用法，前 $n-k$ 位作为一致校验位，后 k 位作为信息位。我们称以式（4-17）为生成矩阵的循环码为**系统循环码**。

例 4.5.2 仍考虑例 4.5.1 中由 $g(x)=1+x+x^3$ 生成的循环码 C。因为

$$x^3=g(x)\cdot 1+(1+x)$$

$$x^4=g(x)\cdot x+(x+x^2)$$

$$x^5=g(x)(x^2+1)+(1+x+x^2)$$

$$x^6=g(x)(x^3+x+1)+(1+x^2)$$

所以，C 作为系统码时的生成矩阵为

$$G=\begin{pmatrix} (1+x)+x^3 \\ (x+x^2)+x^4 \\ (1+x+x^2)+x^5 \\ (1+x^2)+x^6 \end{pmatrix}$$

$$=\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

例如，设$m=(1\ 0\ 1\ 1)$是待编码的消息，于是根据上述生成矩阵，它所对应的码向量为

$$(1\ 1\ 0\ 1\ 0\ 0\ 0)+(1\ 1\ 1\ 0\ 0\ 1\ 0)+(1\ 0\ 1\ 0\ 0\ 0\ 1)$$
$$=(1\ 0\ 0\ 1\ 0\ 1\ 1)$$

可见码字的后 4 位是信息位。

例 4.5.3　令$q=3$，$n=4$。在$GF(3)$上有

$$x^4-1=(x-1)(x+1)(x^2+1)$$

取$g(x)=1+x$，我们就得到一个生成矩阵为

$$G=\begin{pmatrix}1 & 1 & 0 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 1\end{pmatrix}$$

的三元（4，3）循环码。由于$h(x)=(x-1)(x^2+1)=x^3+2x^2+x+2$，故该循环码的一致校验矩阵为

$$H=(1\ 2\ 1\ 2)$$

根据欧几里德除法，显然有

$$x=g(x)\cdot 1+2$$
$$x^2=g(x)(x+2)+1$$
$$x^3=g(x)(x^2+2x+1)+2$$

因此该三元（4，3）循环码作为系统码的生成矩阵为

$$G'=\begin{pmatrix}-2+x\\ -1+x^2\\ -2+x^3\end{pmatrix}=\begin{pmatrix}1 & 1 & 0 & 0\\ 2 & 0 & 1 & 0\\ 1 & 0 & 0 & 1\end{pmatrix}$$

并且与G'对应的一致校验矩阵为

$$H'=(1\ -1\ -2\ -1)=(1\ 2\ 1\ 2)=H$$

例如，待编码的消息为$m=(1\ 2\ 1)$，则它所对应的码字是

$$(1\ 1\ 0\ 0)+(1\ 0\ 2\ 0)+(1\ 0\ 0\ 1)=(0\ 1\ 2\ 1)$$

可见码字的后 3 位是信息位。

§4.6 循环码的若干性质

定义 4.6.1 称多项式

$$x^{\deg f(x)} f\left(\frac{1}{x}\right)$$

为多项式 $f(x)$ 的**互反多项式**，并记为 $\tilde{f}(x)$。

显然，若

$$f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$$

则

$$\begin{aligned}\tilde{f}(x)&=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n\\&=a_n+a_{n-1}x+\cdots+a_1x^{n-1}+a_0x^n\end{aligned}$$

注意到 (n, k) 循环码 C 的一致校验矩阵 H 是其对偶码 $C^\perp$ 的生成矩阵，且 C 的校验多项式 $h(x)$ 的互反多项式 $\tilde{h}(x)$ 即为 $C^\perp$ 的生成多项式。因此根据上一节的结果，我们有

定理 4.6.1 设 $g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}$，$h(x)=h_0+h_1x+\cdots+h_kx^k$，且在 FG 中，$x^n-1=g(x)h(x)$。于是 (n, k) 循环码 $C=\langle g(x)\rangle$ 的对偶码是 $(n, n-k)$ 循环码 $C^\perp=\langle\tilde{h}(x)\rangle$。

下面的事实告诉我们，由循环码的生成多项式往往能够提取有关循环码的重要信息。

定理 4.6.2 设 $C_1=\langle g_1(x)\rangle$，$C_2=\langle g_2(x)\rangle$ 是两个循环码。于是，$C_1\subseteq C_2$ 当且仅当

$$g_2(x)|g_1(x)$$

证明 设 $C_1\subseteq C_2$，则因 $g_1(x)\in C_1$，故 $g_1(x)\in C_2$，因而 $g_1(x)=r(x)g_2(x)$，即 $g_2(x)|g_1(x)$。反之，设 $g_2(x)|g_1(x)$，即 $g_1(x)=s(x)g_2(x)$。对于任意 $a(x)=f(x)g_1(x)\in C_1$，皆有 $a(x)=f(x)s(x)g_2(x)\in C_2$，故 $C_1\subseteq C_2$。

（证毕）

这一定理的直接结果是

定理 4.6.3 设 $x^n-1=g(x)h(x)$ 在 FG 中成立。于

是循环码$C=\langle g(x)\rangle$是自正交码当且仅当

$$\tilde{h}(x)|g(x)$$

证明 注意到自正交码C的定义是$C\subseteq C^{\perp}$，且$C^{\perp}=\langle\tilde{h}(x)\rangle$，则由定理4.6.2立得本定理。〈证毕〉

上面的定理是很有用的，它向我们提供了一种由生成多项式和校验多项式判别循环码是否为自正交码的简单易行的方法。

例4.6.1 设$n=7$，在$GF(2)$上有

$$x^7-1=(x+1)(x^3+x+1)(x^3+x^2+1)$$

我们考虑以

$$g_1(x)=(x+1)(x^3+x+1)$$

为生成多项式的（7，3）循环码C_1，并将它和例4.5.1中的（7，4）循环码$C=\langle g(x)\rangle=\langle x^3+x+1\rangle$作一比较。

由于$g(x)|g_1(x)$，故由定理4.6.2得

$$C_1\subseteq C$$

不仅如此，因为C_1的校验多项式$h_1(x)=x^3+x^2+1$，故$\tilde{h}_1(x)=x^3+x+1=g(x)$。因此

$$C=C_1^{\perp}$$

即

$$C_1\subseteq C_1^{\perp}$$

这表明，C_1是自正交码。

由于$\tilde{h}_1(x)|g_1(x)$，根据定理4.6.3也可以得出同样结果。

定理4.6.4 设$C_1=\langle g_1(x)\rangle$和$C_2=\langle g_2(x)\rangle$是两个循环码，则$C=C_1\cap C_2$也是循环码，并且

$$C=\langle g(x)\rangle$$

其中$g(x)=[g_1(x),\ g_2(x)]$。

证明，由定理4.5.1，要证明C是循环码，我们只需证明C是FG中的一个理想。由于$0\in C_1\cap C_2$，故C不是空集。任取$a(x)$，$b(x)\in C_1\cap C_2$，因为C_1和C_2是理想，故$a(x)-b(x)\in C_1$且$a(x)-b(x)\in C_2$，从而$a(x)-b(x)\in C_1\cap C_2$。又设$p(x)\in FG$，则$p(x)a(x)\in C_1$且$p(x)a(x)\in$

C_2，故 $p(x)a(x)\in C_1\cap C_2$。因此 $C=C_1\cap C_2$ 是 FG 中的理想。

今设 $C=\langle g(x)\rangle$，其中 $g(x)=[g_1(x),\ g_2(x)]$，我们证明 $C=C_1\cap C_2$。因为

$$g(x)=p(x)g_1(x),\quad g(x)=q(x)g_2(x)$$

对于任意 $a(x)=f(x)g(x)\in C$，我们有

$$a(x)=f(x)p(x)g_1(x)\in C_1$$
$$a(x)=f(x)q(x)g_2(x)\in C_2$$

因此 $a(x)\in C_1\cap C_2$，即 $C\subseteq C_1\cap C_2$

反之设 $a(x)\in C_1\cap C_2$，则

$$a(x)=f(x)g_1(x)=h(x)g_2(x)$$

故 $g_1(x)|a(x)$，$g_2(x)|a(x)$，即 $a(x)$ 是 $g_1(x)$ 和 $g_2(x)$ 的公倍式。因而 $g(x)|a(x)$，即 $a(x)=r(x)g(x)\in C$。所以 $C_1\cap C_2\subseteq C$。定理得证。〈证毕〉

回忆 $C_1+C_2\triangleq\{a(x)+b(x)|a(x)\in C_1,\ b(x)\in C_2\}$，我们有

定理 4.6.5 设 $C_1=\langle g_1(x)\rangle$ 和 $C_2=\langle g_2(x)\rangle$ 是两个循环码，则 $C=C_1+C_2$ 也是循环码。并且

$$C=\langle g(x)\rangle$$

其中 $g(x)=(g_1(x),\ g_2(x))$

证明 显然 C 不是空集。任取 $a(x)=\alpha_1(x)+\beta_1(x)$，$b(x)=\alpha_2(x)+\beta_2(x)\in C_1+C_2$，其中 $\alpha_1(x)$，$\alpha_2(x)\in C_1$，$\beta_1(x)$，$\beta_2(x)\in C_2$。于是 $a(x)-b(x)=(\alpha_1(x)-\alpha_2(x))+(\beta_1(x)-\beta_2(x))\in C_1+C_2$。设 $p(x)\in FG$，则 $p(x)a(x)=p(x)\alpha_1(x)+p(x)\beta_1(x)\in C_1+C_2$。因此 $C=C_1+C_2$ 是 FG 中的一个理想，从而是循环码。

设 $C=\langle g(x)\rangle$，其中 $g(x)=(g_1(x),\ g_2(x))$，我们证明 $C=C_1+C_2=\langle g'(x)\rangle$。因为

$$g_1(x)=p(x)g(x),\quad g_2(x)=q(x)g(x),$$

对于任意 $a(x)=f(x)g_1(x)+h(x)g_2(x)\in C_1+C_2$，

我们有

$$a(x)=(f(x)p(x)+h(x)q(x))g(x)\in C$$

因此 $C_1+C_2\subseteq C$

反之，由 $C_1\subseteq C_1+C_2$ 和 $C_2\subseteq C_1+C_2$，我们有

$g'(x)|g_1(x)$，$g'(x)|g_2(x)$

因此，$g'(x)|g(x)$，故 $C\subseteq C_1+C_2$。 〈证毕〉

例 4.6.2 再看例 4.5.3，设 $C_1=\langle 1+x\rangle$，其生成矩阵为

$$G_1=\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

设 $C_2=\langle (x-1)(x+1)\rangle=\langle x^2+2\rangle$，其生成矩阵为

$$G_2=\begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{pmatrix}$$

由于 $(1+x)|(x^2+2)$，故 $C_2\subseteq C_1$。事实上，G_2 的第 1 行是 G_1 的第 1 行乘 2 与第 2 行之和；G_2 的第 2 行是 G_1 的第 2 行乘 2 与第 3 行之和。因此的确有 $C_2\subseteq C_1$。

由于 $[1+x, x^2+1]=x^2+1$，$(1+x, x^2+1)=1+x$，故 $C_1\cap C_2=\langle x^2+1\rangle$，$C_1+C_2=\langle 1+x\rangle$。因为 $C_2\subseteq C_1$，故 $C_1\cap C_2=C_2$，$C_1+C_2=C_1$，所以上述结果是必然的。

在本节的末尾，我们考虑最常用的二元循环码。由于 $(n, 2)=1$，故码长 n 为奇数。

在 $GF(2)$ 上，我们有

$$x^n-1=(1+x)(1+x+\cdots+x^{n-1})$$

$C=\langle 1+x\rangle$是 $(n, n-1)$ 循环码。因为 $1+x+\cdots+x^{n-1}$ 的互反多项式就是它自己，所以 $C^{\perp}=\langle 1+x+\cdots+x^{n-1}\rangle$。$C^{\perp}$ 是 1 维循环码，只有两个码向量，即零向量和全 1 向量 $\boldsymbol{h}$。因此一个二元向量和 $\boldsymbol{h}$ 正交当且仅当该二元向量的重量是偶数。

综上所述，我们有

定理 4.6.6 二元 $(n, n-1)$ 循环码 $C=\langle 1+x\rangle$由全

体n长的偶重量向量组成。

推论4.6.6.1 二元循环码$C=\langle g(x)\rangle$仅含有偶重量向量当且仅当$(1+x)|g(x)$。

证明 $C=\langle g(x)\rangle$中仅含有偶重量向量当且仅当$C\subseteq\langle 1+x\rangle$当且仅当$(1+x)|g(x)$。 〈证毕〉

推论4.6.6.2 若二元循环码$C=\langle g(x)\rangle$是自正交码，则$(1+x)|g(x)$。

证明 二元自正交码仅由偶重量向量组成。因此，$(1+x)|g(x)$。 〈证毕〉

注意，上述推论之逆不真。

例4.5.2中的二元(7，4)循环码$C=\langle 1+x+x^3\rangle$中含有奇重量向量，因为$(1+x)\nmid(1+x+x^3)$。而例4.6.1中的二元(7，3)循环码$C_1=\langle(x+1)(x^3+x+1)\rangle$，则仅含偶重量向量。事实上，它还是自正交码。

第五章 有 限 域

§5.1 有限域的乘法结构

定义5.1.1 由有限个元素的集合所构成的域称为**有限域**或**伽罗瓦（Galois）域**。域中元素的个数称为该有限域的阶。用符号$GF(q)$表示q阶有限域。

例如，由0，1两个元素所构成的二元域即为二元有限域，记为$GF(2)$。又如，模p整数所构成的剩余类集合（p为素数）

$$\{\bar{0},\ \bar{1},\ \bar{2},\ \cdots,\ \overline{p-1}\}$$

构成p阶有限域$GF(p)$。

以后我们要讲到有限域$GF(q)$的阶必为某一素数之幂p^m（m为正整数）。

我们知道一个域中所有非零元素的集合构成阿贝尔乘法群。对于q阶有限域$GF(q)$，它的所有非零元素的集合关于域中乘法构成$q-1$阶有限群。

回忆乘法群中有限阶的元素α，其阶为使

$$\alpha^n = 1$$

的最小正整数n。一个群中的n阶元素α生成一个n阶循环群，即

$$\langle\alpha\rangle = \{1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{n-1}\}$$

我们将域中非零元素关于域的乘法群的阶定义为域中**非零元素的阶**。

在§3.4中，我们曾指出过n阶有限群中的任意元素a均满足等式

$$a^n = 1$$

特别有限域 $GF(q)$ 的 $q-1$ 阶乘法群中的任意元素 a 均满足等式

$$a^{q-1}=1$$

换言之，$GF(q)$ 中的任意非零元素都满足方程

$$x^{q-1}-1=0$$

若把 $GF(q)$ 中的零元素也考虑进去，我们断定 $GF(q)$ 中的任意元素皆满足方程

$$x^q-x=0$$

因此得

定理5.1.1 q 阶有限域 $GF(q)$ 中的任意非零元素均满足方程

$$x^{q-1}-1=0 \tag{5-1}$$

而 q 阶有限域 $GF(q)$ 中的任意元素均满足方程

$$x^q-x=0 \tag{5-2}$$

换言之，q 阶有限域 $GF(q)$ 可视为方程（5-2）的全部根的集合。

定义5.1.2 若域中元素 α 是 n 阶的，则称 α 是**n次单位原根**，简称为**n次原根**。一般若域中元素 α 满足等式 $\alpha^n=1$，则称 α 为n次单位根。若在 q 阶有限域 $GF(q)$ 中存在 $q-1$ 阶元素 α 时，则称 α 为 $GF(q)$ **的本原域元素**，简称**本原元**。

显然，若 q 阶有限域 $GF(q)$ 存在本原元 α，则 $GF(q)$ 的全体非零元素构成一个由 α 生成的 $q-1$ 阶循环群。因此 q 阶有限域 $GF(q)$ 的本原元实际上是 $GF(q)$ 的 $q-1$ 阶乘法群的生成元。这样一来 $GF(q)$ 的全部元素可以明确地表示为

$$GF(q)=\{0,\ 1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{q-2}\}$$

定理5.1.2 q 阶有限域 $GF(q)$ 中一定含有本原元。

证明　方法1 $q=2$ 时，定理显然成立。设 $q>2$。假定

$$q-1=\prod_{i=1}^{m} q_i^{e_i}$$

是 $q-1$ 的素因子分解式。由定理 3.1.12，在 $GF(q)$ 内，方程

$$x^{\frac{q-1}{q_i}} - 1 = 0$$

至多有$\frac{q-1}{q_i}$个根。于是在 $GF(q)$ 内至多有$\frac{q-1}{q_i}$个元素 a 满足

$$a^{\frac{q-1}{q_i}} = 1$$

由于 $GF(q)$ 中有 $q-1$ 个非零元素，而$\frac{q-1}{q_i} < q-1$，因此存在 $a_i \neq 0 \in GF(q)$，使

$$a_i^{\frac{q-1}{q_i}} \neq 1$$

现在我们断言，域元素 $b_i = a_i^{\frac{q-1}{q_i^{e_i}}}$ 阶为 $q_i^{e_i}$。由定理5.1 1

$$b_i^{q_i^{e_i}} = a_i^{q-1} = 1$$

因此根据定理 3.3.5，若设 b_i 之阶为 λ_i，则必有

$$\lambda_i \mid q_i^{e_i}$$

因此 $\lambda_i = q_i^{\mu_i}$，其中 $0 \leqslant \mu_i \leqslant e_i$。另一方面，因为

$$b_i^{q_i^{e_i-1}} = \left(a_i^{\frac{q-1}{q_i^{e_i}}} \right)^{q_i^{e_i-1}} = a_i^{\frac{q-1}{q_i}} \neq 1 \tag{5-3}$$

故 $\mu_i = e_i$。否则，若 $0 \leqslant \mu_i \leqslant e_i - 1$ 则

$$b_i^{q_i^{e_i-1}} = \left(b_i^{q_i^{\mu_i}} \right)^{q_i^{e_i-1-\mu_i}} = 1$$

此与式（5-3）矛盾。因此 b_i 的阶为 $q_i^{e_i}$。

作

$$\alpha = \prod_{i=1}^{m} b_i$$

显然 $\alpha \in GF(q)$。由定理 3.3.6，α 的阶为

$$\prod_{i=1}^{m} q_i^{e_i} = q - 1$$

方法 2 设 α 是 $GF(q)$ 中具有最大阶 r 的元素。由于 1，α，α^2，…，α^{r-1} 互不相同且不为零，故 $r \leqslant q-1$。

任取 $\beta \neq 0 \in GF(q)$，设 β 的阶为 s，我们断言，$s \mid r$。对于任意素数 p，如果 $r = p^a r'$，$s = p^b s'$，其中 $p \nmid r'$，$p \nmid s'$。于是，由定理 3.3.7，α^{p^a} 的阶为

$$\frac{p^a r'}{(p^a r', p^a)} = \frac{p^a r'}{p^a} = r'$$

同理，$\beta^{s'}$ 的阶为 p^b。因为 $(r', p^b) = 1$，故由定理 3.3.6，$\alpha^{p^a}\beta^{s'}$ 的阶为 $p^b r'$，由假定，$r = p^a r'$ 是最大阶，因此 $b \leqslant a$。这表明，任何能整除 s 的素数幂都能整除 r，故 $s \mid r$。于是，任意 $\beta \neq 0 \in GF(q)$ 都是方程 $x^r - 1 = 0$ 的根。由此可得

$$\prod_{\substack{\beta \in GF(q) \\ \beta \neq 0}} (x - \beta) \mid (x^r - 1)$$

但 $\Pi(x-\beta)$ 是 $q-1$ 次多项式，故 $r \geqslant q-1$。因此 $r = q-1$。 〈证毕〉

上述定理告诉我们，对于有限域，它的非零元素全体不仅构成一个阿贝尔乘法群，而且还构成一个循环群。这就是有限域较之无限域的最大优越性所在。

我们再作一个注记。$GF(q)$ 中的本原元不只有一个（当 $q > 2$ 时）。设 α 是本原元，对于任意 $1 \leqslant n \leqslant q-1$，只要 $(n, q-1) = 1$，则由定理 3.3.7，α^n 的阶亦为

$$\frac{q-1}{(n, q-1)} = q - 1$$

即 α^n 也是本原元。因此 $GF(q)$ 上的本原元共有 $\varphi(q-1)$ 个。关于欧拉函数 $\varphi(n)$ 我们已在 § 3.2 中给出过定义，并将在下一节详细介绍。

最后我们指出，若α是$GF(q)$的本原元，则x^q-x在$GF(q)$中可完全分解成下述一次因式：

$$x^q - x = x\prod_{i=0}^{q-2}(x-\alpha^i)$$

§5.2 数论函数

为了进一步阐述有限域的理论，我们需要用到一些重要的数论函数，主要是麦比乌斯（Möbius）函数和欧拉函数。

定义5.2.1 若$f(n)$是对于一切正整数n都有定义的函数，则称$f(n)$为数论函数。

我们感兴趣的是下面一类特殊的数论函数。

定义5.2.2 设$f(n)\neq 0$是数论函数。若$(m, n)=1$，则$f(mn)=f(m)f(n)$，称$f(n)$为**积性函数**。如果取消条件$(m, n)=1$的限制，即恒有$f(mn)=f(m)f(n)$，则称$f(n)$为**完全积性函数**。

例5.2.1 函数

$$\Delta(n)=\begin{cases}1, & 若\ n=1\\ 0, & 若\ n\neq 1\end{cases}$$

是完全积性函数。事实上

$$\Delta(mn)=\Delta(m)\Delta(n) \tag{5-4}$$

恒成立，因为当$m=n=1$时，式（5-4）两边均为1；其它情形则式（5-4）两边均为0。

例5.2.2 麦比乌斯函数

$$\mu(n)=\begin{cases}1, & 若\ n=1\\ (-1)^k, & 若\ n\ 为\ k\ 个不同素数的乘积\\ 0, & 若\ n\ 含有平方因子\end{cases}$$

是积性函数，但不是完全积性函数

设$(m, n)=1$，不妨令$m\neq 1$，$n\neq 1$，且m与n均不含平方因子。因为上述情形

$$\mu(mn)=\mu(m)\mu(n)$$

显然成立。因此m和n的素因子分解式可写成

$$m=p_1\cdots p_r,\quad n=q_1\cdots q_s$$

其中$p_i\neq q_j$。于是

$$\mu(mn)=(-1)^{r+s}=(-1)^r(-1)^s=\mu(m)\mu(n)$$

写出$\mu(n)$的前几项

$\mu(1)=1$，　　$\mu(2)=-1$，　　$\mu(3)=-1$，

$\mu(4)=0$，　　$\mu(5)=-1$，　　$\mu(6)=1$，

$\mu(7)=-1$，　　$\mu(8)=0$，　　$\mu(9)=0$，

$\mu(10)=1$，　　$\mu(11)=-1$，　　$\mu(12)=0$，…

由此可见$\mu(n)$不是完全积性函数。

积性函数$f(n)$的优点在于，若n的素因子分解式为$n=p_1^{\alpha_1}\cdots\cdots p_k^{\alpha_k}$，则

$$f(n)=f(p_1^{\alpha_1})\cdots f(p_k^{\alpha_k})$$

即若已知$f(n)$，当n为素数幂时之值，则$f(n)$已经完全确定。当$f(n)$为完全积性函数时，更有

$$f(n)=f(p_1)^{\alpha_1}\cdots f(p_k)^{\alpha_k}$$

即若已知$f(n)$，当n为素数时的值，则$f(n)$已经完全确定。

积性函数有如下的重要性质。

性质1　设$f(n)$为积性函数，则$f(1)=1$。

证明　因为$f(n)\not\equiv 0$，故存在m，使$f(m)\neq 0$。因此，

$$f(m)=f(1\cdot m)=f(1)f(m)$$

从而$f(1)=1$。　　〈证毕〉

性质2　设$f_1(n)$，$f_2(n)$为积性函数，则$f(n)=f_1(n)f_2(n)$也是积性函数。

证明　$f(1)=f_1(1)f_2(1)=1$，故$f(n)\not\equiv 0$。此外当$(n,m)=1$时

$$\begin{aligned}f(nm)&=f_1(nm)f_2(nm)=f_1(n)f_1(m)f_2(n)f_2(m)\\&=(f_1(n)f_2(n))(f_1(m)f_2(m))=f(n)f(m)\end{aligned}$$

〈证毕〉

类似地我们有：若 $f_1(n)$，$f_2(n)$ 为完全积性函数，则 $f(n)=f_1(n)f_2(n)$ 也是完全积性函数。其证明几乎是完全相同的。

性质 3 设 $f(n)$ 为积性函数，$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 n 的标准素因子分解式，则

$$\sum_{d\mid n} f(d)=\prod_{i=1}^{k}(1+f(p_i)+\cdots+f(p_i^{\alpha_i}))$$

式 $\sum\limits_{d\mid n} f(d)$ 表示对 n 的所有正因子 d 求 $f(d)$ 之和。

证明 显然 n 的全体正因子为

$p_1^{\beta_1}\cdots p_k^{\beta_k}$，$0\leqslant\beta_i\leqslant\alpha_i$，$i=1$，…，$k$

因此

$$\begin{aligned}\sum_{d\mid n} f(d)&=\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_k=0}^{\alpha_k} f(p_1^{\beta_1}\cdots p_k^{\beta_k})\\&=\sum_{\beta_1=0}^{\alpha_1}\cdots\sum_{\beta_k=0}^{\alpha_k} f(p_1^{\beta_1})\cdots f(p_k^{\beta_k})\\&=\sum_{\beta_1=0}^{\alpha_1} f(p_1^{\beta_1})\cdots\sum_{\beta_k=0}^{\alpha_k} f(p_k^{\beta_k})\\&=(f(p_1^0)+\cdots+f(p_1^{\alpha_1}))\cdots(f(p_k^0)\\&\quad+\cdots+f(p_k^{\alpha_k}))\\&=\prod_{i=1}^{k}(f(p_i^0)+f(p_i)+\cdots+f(p_i^{\alpha_i}))\end{aligned}$$

注意到 $f(p_i^0)=f(1)=1$，故得所欲证。〈证毕〉

特别若取 $f(n)=1$，则有

$$\tau(n)\triangleq\sum_{d\mid n}1=\prod_{i=1}^{k}(1+\alpha_i)$$

在§3.3中，$\tau(n)$ 表示 n 的正因子的个数。由此可见 $\tau(n)$ 是积性函数。设 $(n, m)=1$，且 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，$m=q_1^{\beta_1}\cdots q_l^{\beta_l}$，

其中，$p_i \neq q_i$。于是，

$$\tau(mn) = \prod_{i=1}^{k}(1+\alpha_i)\prod_{j=1}^{l}(1+\beta_j) = \tau(m)\tau(n)$$

极易算出

$$\tau(1)=1,\quad \tau(2)=2,\quad \tau(3)=2,$$
$$\tau(4)=3,\quad \tau(5)=2,\quad \tau(6)=4,$$
$$\tau(7)=2,\quad \tau(8)=4,\quad \tau(9)=3,\quad \cdots$$

由此可见 $\tau(n)$ 不是完全积性函数。我们常称 $\tau(n)$ 为除数函数，是一种重要的数论函数。

下面讨论麦比乌斯函数的重要性质。

定理5.2.1 设 $f(n)$ 为积性函数，$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 n 的标准素因子分解式，则

$$\sum_{d\mid n}\mu(d)f(d) = \prod_{i=1}^{k}(1-f(p_i)) \tag{5-5}$$

证明 由性质2，$\mu(n)f(n)$ 是积性函数。再由性质3，我们有

$$\sum_{d\mid n}\mu(d)f(d) = \prod_{i=1}^{k}(1+\mu(p_i)f(p_i) + \cdots + \mu(p_i^{\alpha_i})f(p_i^{\alpha_i}))$$

注意到

$$\mu(p_i) = -1,\quad \mu(p_i^2) = \cdots = \mu(p_i^{\alpha_i}) = 0$$
$$i=1,\ 2,\ \cdots,\ k$$

故定理得证。 〈证毕〉

特别在式（5-5）中令 $f(n)=1$，则

$$\Delta(n) \triangleq \sum_{d\mid n}\mu(d) = \begin{cases} 1, & 若\ n=1 \\ 0, & 若\ n\neq 1 \end{cases} \tag{5-6}$$

若令 $f(n)=\dfrac{1}{n}$，则得

$$\sum_{d|n}\frac{\mu(d)}{d}=\begin{cases}1 & ，若 n=1\\ \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) & ，若 n\neq 1\end{cases} \tag{5-7}$$

定义5.2.3 假定

$$g(n)=\sum_{d|n}f(d)=\sum_{d|n}f\left(\frac{n}{d}\right)$$

则称 $g(n)$ 为 $f(n)$ 的麦比乌斯变换，而 $f(n)$ 则称为 $g(n)$ 的麦比 斯逆变换。

注意我们总可以将 $\sum_{d|n}f(d)$ 写成 $\sum_{d|n}f\left(\frac{n}{d}\right)$，因为当 d 遍历 n 的一切正因子时，$\frac{n}{d}$ 也遍历 n 的一切正因子。

因此函数 $\Delta(n)$ 是麦比乌斯函数 $\mu(n)$ 的麦比乌斯变换，而 $\mu(n)$ 是 $\Delta(n)$ 的麦比乌斯逆变换。

下述定理是十分重要的，在编码理论中也经常用到。

定理5.2.2 （麦比乌斯反转公式）

设

$$g(n)=\sum_{d|n}f(d) \tag{5-8}$$

则

$$f(n)=\sum_{d|n}\mu(d)g\left(\frac{n}{d}\right) \tag{5-9}$$

反之由式（5-9）也可以推出式（5-8）。

证明 设 $d|n$，则由式（5-8）可得

$$g\left(\frac{n}{d}\right)=\sum_{d'|\frac{n}{d}}f(d')$$

于是

$$\sum_{d\mid n}\mu(d)g\left(\frac{n}{d}\right)=\sum_{d\mid n}\mu(d)\sum_{d'\mid\frac{n}{d}}f(d') \qquad (5\text{-}10)$$

将式（5-10）的右边展开，并按照 $f(d')$ 归并同类项（亦即改变求和次序）。写 $n=dd'n_1$，注意到对于 n 的任意正因子 d'，d 遍历 $\frac{n}{d'}$ 的一切正因子，因而有

$$\sum_{d\mid n}\mu(d)\sum_{d'\mid\frac{n}{d}}f(d')=\sum_{d'\mid n}f(d')\sum_{d\mid\frac{n}{d'}}\mu(d)$$

再由式（5-6），我们有

$$\sum_{d'\mid n}f(d')\sum_{d\mid\frac{n}{d'}}\mu(d)=f(n)$$

因此式（5-9）成立。

同理，由式（5-9）可以推出式（5-8）。 〈证毕〉

为了理解这一定理的证明，我们举一个例子。

例5.2.3 设 $n=4$，于是

$$\sum_{d\mid n}\mu(d)\sum_{d'\mid\frac{n}{d}}f(d')=\mu(1)\{f(1)+f(2)+f(4)\}$$
$$+\mu(2)\{f(1)+f(2)\}$$
$$+\mu(4)\{f(1)\}$$

改变上式之求和顺序，按 $f(1)$，$f(2)$，$f(4)$ 归并同类项，则有

$$f(1)\{\mu(1)+\mu(2)+\mu(4)\}$$
$$+f(2)\{\mu(1)+\mu(2)\}$$
$$+f(4)\{\mu(1)\}=\sum_{d'\mid n}f(d')\sum_{d\mid\frac{n}{d'}}\mu(d)$$

在结束本节之前，我们考虑另一个重要的数论函数，即欧拉函数，它的定义已在§ 3.2 中给出过，并曾多次用到。

我们根据$d=(n, a)$将正整数1，2，…，a，…，n加以分类，即若a适合$d=(n, a)$，则将a归入d类。显然共有$\tau(n)$个类。那么，每一类中各有多少个正整数呢？由于$\left(\frac{n}{d}, \frac{a}{d}\right)=1$，当且仅当$d=(n, a)$，故$d$类中共有$\varphi\left(\frac{n}{d}\right)$个正整数。因此

$$n=\sum_{d \mid n} \varphi\left(\frac{n}{d}\right)=\sum_{d \mid n} \varphi(d)$$

由此可见n是欧拉函数$\varphi(n)$的麦比乌斯变换。

由麦比乌斯反转公式立得

$$\varphi(n)=n \sum_{d \mid n} \frac{\mu(d)}{d}$$

再根据式（5-7），我们进一步有

$$\varphi(n)=n \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)=p_1^{\alpha_1} \cdots p_k^{\alpha_k} \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

$$=\prod_{i=1}^{k}\left(p_i^{\alpha_i}-p_i^{\alpha_i-1}\right)$$

其中$n=p_1^{\alpha_1} \cdots p_k^{\alpha_k}$。

从上述公式很容易推断出$\varphi(n)$是积性函数。设$(m, n)=1$，且$m=p_1^{\alpha_1} \cdots p_k^{\alpha_k}$，$n=q_1^{\beta_1} \cdots q_l^{\beta_l}$，其中$p_i \neq q_j$。于是$mn$的素因子分解式为

$$mn=p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$$

因此

$$\varphi(mn)=mn \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \prod_{j=1}^{l}\left(1-\frac{1}{q_j}\right)$$

$$=\varphi(m) \varphi(n)$$

$\varphi(n)$ 的前几项是

$$\varphi(1)=1,\quad \varphi(2)=1,\quad \varphi(3)=2,$$
$$\varphi(4)=2,\quad \varphi(5)=4,\quad \varphi(6)=2,$$
$$\varphi(7)=6,\quad \varphi(8)=4,\quad \varphi(9)=6,\quad \cdots$$

显然 $\varphi(n)$ 不是完全积性函数。

综上所述，我们有

定理5.2.3 欧拉函数 $\varphi(n)$ 是积性函数，并且下述关系式成立：

$$n=\sum_{d\mid n}\varphi(d)=\sum_{d\mid n}\varphi\left(\frac{n}{d}\right) \tag{5-11}$$

$$\varphi(n)=n\sum_{d\mid n}\frac{\mu(d)}{d} \tag{5-12}$$

$$=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) \tag{5-13}$$

$$=\prod_{i=1}^{k}\left(p_i^{\alpha_i}-p_i^{\alpha_i-1}\right)$$

其中 n 的素因子分解式为 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$

例5.2.4 设 $n=12$，依 $d=(12,a)$ 将 $1,2,\cdots,a,\cdots,12$ 分为 $\tau(12)=\tau(2^2\cdot 3)=(1+2)(1+1)=6$ 类，如表 5-1 所示。

表 5-1

d	a	$\varphi\left(\frac{12}{d}\right)$
1	1,5,7,11	$\varphi(12)=4$
2	2,10	$\varphi(6)=2$
3	3,9	$\varphi(4)=2$
4	4,8	$\varphi(3)=2$
6	6	$\varphi(2)=1$
12	12	$\varphi(1)=1$

§5.3 分圆多项式

我们知道（n，k）循环码的生成多项式是x^n-1的因式。因此求生成多项式必须将x^n-1分解因式。这是一个很困难的问题，分圆多项式提供了解决这个问题的一种途径。

首先我们介绍分圆多项式的来历。在例3.3.1中，我们曾经指出，复数域上的n次方程

$$Z^n-1=0$$

的全部根构成一个n阶循环群U_n：

$$1,\quad \varepsilon=e^{\frac{2\pi}{n}i},\quad \varepsilon^2=e^{\frac{4\pi}{n}i},\quad \cdots\varepsilon^{n-1}=e^{\frac{2(n-1)\pi}{n}i}$$

这n个根刚好代表坐标平面上以原点为中心的单位圆内接正多边形的n个顶点。例如，我们研究4次方程

$$Z^4-1=0$$

它的4个根

$$1,\quad \varepsilon=e^{\frac{2\pi}{4}i}=i,\quad \varepsilon^2=i^2=-1,\quad \varepsilon^3=-i$$

位于图5-1中单位圆内接正4边形的顶点上。这4个根中，1为1阶元素，-1为2阶元素，i和$-i$为4阶元素。在分解式

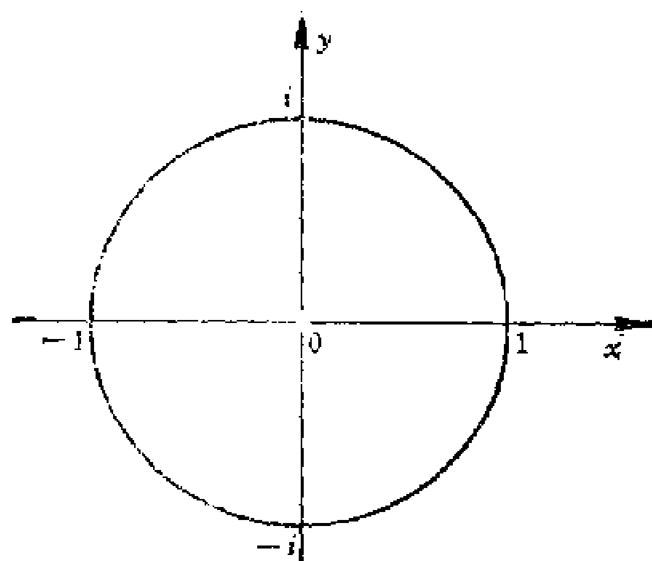

图 5-1

$$Z^4-1=(Z-1)(Z+1)(Z-i)(Z+i)$$

中把同阶的元素集合在一起，可写成

$$Z^4-1=Q^{(1)}(Z)Q^{(2)}(Z)Q^{(4)}(Z)$$

其中 $Q^{(1)}(Z)=Z-1$，$Q^{(2)}(Z)=Z+1$，$Q^{(4)}(Z)=Z^2+1$。我们称 $Q^{(1)}(Z)$，$Q^{(2)}(Z)$，$Q^{(4)}(Z)$ 为分圆多项式。

现在我们讨论任意域上分圆多项式的概念。

假定 α 是某一个域中的 n 阶元素。于是 1，α，…，α^{n-1} 就是方程

$$x^n-1=0$$

的全部根。根据定理 3.1.12，x^n-1 在任一域上至多有 n 个根。因此得

定理5.3.1 在含有 n 阶元素的任意域上，恒有下述因式分解

$$x^n-1=\prod_{i=0}^{n-1}(x-\alpha^i)=\prod_{i=1}^{n}(x-\alpha^i)$$

其中 α 为域中的一个 n 阶元素。

对于给定的 n，是否一定有包含 n 阶元素的有限域呢？以后我们要讲到，当 $(n,\ p)=1$ 时，包含 n 阶元素的有限域一定存在，此处 p 代表该有限域的特征，其含意将在下一节介绍。

在含有 n 阶元素的域上，方程 $x^n-1=0$ 的任意根的阶都能整除 n。设 α 为域中的 n 阶元素，则 x^n-1 的每一个根都为 α 的某次幂 α^i，而根据定理 3.3.7，α^i 的阶为 $\frac{n}{(i,\ n)}$。反过来，每一个阶能整除 n 的域元素都是方程 $x^n-1=0$ 的根。若 β 为 d 阶元素，则 $n=n_1d$，于是

$$\beta^n=\beta^{n_1d}=(\beta^d)^{n_1}=1$$

综上所述，在含有 n 阶元素的域上，方程 $x^n-1=0$ 的全部根的集合与阶能整除 n 的域元素的集合完全一致。因此我们可以将方程 $x^n-1=0$ 的全部根按照它们的阶加以分类

$$x^n - 1 = \prod_{d \mid n} \prod_{\substack{\beta 为 d 阶 \\ 域元素}} (x - \beta)$$

定义5.3.1 以全体 d 阶元素为根的多项式

$$\prod_{\beta 为 d 阶元素} (x - \beta)$$

称为**分圆多项式**，记为 $Q^{(d)}(x)$。

由此定义及上面的讨论，立得

定理5.3.2 在含有 n 阶元素的域中，下述分圆分解公式成立

$$x^n - 1 = \prod_{d \mid n} Q^{(d)}(x)$$

下述定理是乘积形式的麦比乌斯反转公式，其证明类似于定理5.2.2。为使读者加深对这种证明方法（改变求和或求积顺序）的理解，我们仍然不厌其烦地给出了证明。

定理5.3.3 （麦比乌斯反转公式）

设

$$g(n) = \prod_{d \mid n} f(d) \tag{5-14}$$

则

$$f(n) = \prod_{d \mid n} g\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d \mid n} g(d)^{\mu\left(\frac{n}{d}\right)} \tag{5-15}$$

反之，由式（5-15）也可以推出式（5-14）。

证明 当 $d \mid n$ 时，由式（5-14）可得

$$g\left(\frac{n}{d}\right) = \prod_{d' \mid \frac{n}{d}} f(d')$$

因此

$$\prod_{d\mid n} g\left(\frac{n}{d}\right)^{\mu(d)}=\prod_{d\mid n}\prod_{d'\mid \frac{n}{d}} f(d')^{\mu(d)} \tag{5-16}$$

将式（5-16）展开，并改变其求积顺序，即将具有相同 d' 的 $f(d')$ 写在一起。由于 $n=dd'n_1$，注意到当 d 遍历 n 的一切正因子时，d' 也遍历 n 的一切正因子；并且当 d' 固定时，d 遍历 $\frac{n}{d'}$ 的一切正因子。因而有

$$\prod_{d\mid n}\prod_{d'\mid \frac{n}{d}} f(d')^{\mu(d)}=\prod_{d'\mid n}\prod_{d\mid \frac{n}{d'}} f(d')^{\mu(d)}$$

$$=\prod_{d'\mid n} f(d')^{\sum\limits_{d\mid \frac{n}{d'}}\mu(d)}$$

再由式（5-6），得

$$\prod_{d'\mid n} f(d')^{\sum\limits_{d\mid \frac{n}{d'}}\mu(d)}=f(n)$$

定理的前半部就证明完了。

由式（5-15）可得

$$f\left(\frac{n}{d}\right)=\prod_{d'\mid \frac{n}{d}} g(d')^{\mu\left(\frac{n}{d'd}\right)}$$

因此

$$\prod_{d\mid n} f\left(\frac{n}{d}\right)=\prod_{d\mid n}\prod_{d'\mid \frac{n}{d}} g(d')^{\mu\left(\frac{n}{d'd}\right)}$$

$$=\prod_{d'\mid n}\prod_{d\mid \frac{n}{d'}} g(d')^{\mu\left(\frac{n}{d'd}\right)}$$

$$=\prod_{d'|n} g(d')^{\sum_{d|\frac{n}{d'}} \mu\left(\frac{n}{d'd}\right)} = \prod_{d'|n} g(d')^{\sum_{d|\frac{n}{d'}} \mu(d)} = g(n)$$

于是定理的后半部也成立。 〈证毕〉

利用上述麦比乌斯反转公式，我们可以得到分圆多项式 $Q^{(n)}(x)$ 的显式表达式。设 $g(n)=x^n-1$，$f(n)=Q^{(n)}(x)$，根据定理5.3.2有

$$g(n)=\prod_{d|n} f(d)$$

因此

$$f(n)=Q^{(n)}(x)=\prod_{d|n} g(d)^{\mu\left(\frac{n}{d}\right)}=\prod_{d|n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}$$

由此得

定理5.3.4 分圆多项式 $Q^{(n)}(x)$ 可以表示成

$$Q^{(n)}(x)=\prod_{d|n}(x^d-1)^{\mu\left(\frac{n}{d}\right)}=\prod_{d|n}\left(x^{\frac{n}{d}}-1\right)^{\mu(d)} \tag{5-17}$$

为了实际计算分圆多项式，常常需要利用它的许多性质。我们摘要介绍如下。

性质1 设 p 是素数且 $p\nmid m$，则

$$Q^{(mp^k)}(x)=Q^{(pm)}(x^{p^{k-1}})$$

证明 注意到当 d 含平方素因子时，则 $\mu(d)=0$。因此

$$Q^{(mp^k)}(x)=\prod_{d|p^km}\left(x^{\frac{mp^k}{d}}-1\right)^{\mu(d)}$$

$$=\prod_{d|pm}\left[(x^{p^{k-1}})^{\frac{pm}{d}}-1\right]^{\mu(d)}$$

$$=Q^{(pm)}(x^{p^{k-1}})$$

〈证毕〉

由性质1立即可得

性质2 设n的标准因子分解式为$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，则

$$Q^{(n)}(x)=Q^{(p_1\cdots p_k)}\left(x^{\prod\limits_{i=1}^{k}p_i^{\alpha_i-1}}\right)$$

性质3 设p是素数且$p\nmid m$，则

$$Q^{(pm)}(x)=\frac{Q^{(m)}(x^p)}{Q^{(m)}(x)}$$

证明 我们有

$$Q^{(pm)}(x)=\left[\prod_{d|m}\left(x^{\frac{pm}{d}}-1\right)^{\mu(d)}\right]\left[\prod_{\substack{d|pm\\ d\nmid m}}\left(x^{\frac{pm}{d}}-1\right)^{\mu(d)}\right]$$

$$=Q^{(m)}(x^p)\cdot\prod_{\substack{d|pm\\ d\nmid m}}\left(x^{\frac{pm}{d}}-1\right)^{\mu(d)}$$

注意条件$d|pm$且$d\nmid m$等价于条件$k|m$，其中$d=pk$。因此：

$$\prod_{\substack{d|pm\\ d\nmid m}}\left(x^{\frac{pm}{d}}-1\right)^{\mu(d)}=\prod_{k|m}\left(x^{\frac{m}{k}}-1\right)^{\mu(pk)}$$

又由于

$$\mu(pk)=\mu(p)\mu(k)=-\mu(k)$$

最后得

$$\prod_{k|m}\left(x^{\frac{m}{k}}-1\right)^{\mu(pk)}=\prod_{k|m}\left(x^{\frac{m}{k}}-1\right)^{-\mu(k)}=\frac{1}{Q^{(m)}(x)}$$

〈证毕〉

性质4 若$n\geqslant 2$，则

$$Q^{(n)}(x)=\prod_{d|n}\left(1-x^{\frac{n}{d}}\right)^{\mu(d)}$$

证明 因为

$$Q^{(n)}(x)=\prod_{d|n}\left(x^{\frac{n}{d}}-1\right)^{\mu(d)}$$

$$=(-1)^{\sum\limits_{d|n}\mu(d)}\prod_{d|n}\left(1-x^{\frac{n}{d}}\right)^{\mu(d)}$$

$$=\begin{cases}-\prod\limits_{d|n}\left(1-x^{\frac{n}{d}}\right)^{\mu(d)}, & 若 n=1\\ \prod\limits_{d|n}\left(1-x^{\frac{n}{d}}\right)^{\mu(d)}, & 若 n\neq 1\end{cases}$$

（证毕）

性质 5　若 $n\geqslant 3$ 且 n 为奇数，则

$$Q^{(2n)}(x)=Q^{(n)}(-x)$$

证明　由性质 3 和 4 得

$$Q^{(2n)}(x)=\frac{Q^{(n)}(x^2)}{Q^{(n)}(x)}=\prod_{d|n}\left(\frac{1-x^{\frac{2n}{d}}}{1-x^{\frac{n}{d}}}\right)^{\mu(d)}$$

$$=\prod_{d|n}\left(1+x^{\frac{n}{d}}\right)^{\mu(d)}=Q^{(n)}(-x)$$

（证毕）

性质 6　分圆多项式的次数由下述公式确定：

$$\deg Q^{(n)}(x)=\varphi(n)$$

证明　设 α 为 n 阶域元素，于是

α^i 为 n 阶元素当且仅当 $(n,\ i)=1$，$i=1$，…，n。由此可见，在

$$\alpha,\ \alpha^2,\ \cdots,\ \alpha^{n-1},\ \alpha^n=1$$

中共有 $\varphi(n)$ 个 n 阶元素。因此，$\deg Q^{(n)}(x)=\varphi(n)$。

（证毕）

性质 7　当 $n\geqslant 2$ 时，分圆多项式与其互反多项式相等，即

$$Q^{(n)}(x)=\tilde{Q}^{(n)}(x)=x^{\varphi(n)}Q^{(n)}\left(\frac{1}{x}\right)$$

证明 设 α 为 n 阶域元素，则 α^{-1} 亦然。因此，$Q^{(n)}(\alpha^{-1})=0$ 当且仅当 $Q^{(n)}(\alpha)=0$，亦即 $Q^{(n)}(x)$ 与 $\tilde{Q}^{(n)}(x)$ 有相同的根集合。此外，当 $n\geqslant 2$ 时，它们都是首一 $\varphi(n)$ 次多项式。因而

$$Q^{(n)}(x)=x^{\varphi(n)}Q^{(n)}\left(\frac{1}{x}\right)$$

并且

$$Q^{(n)}(x)=\sum_{i=0}^{\varphi(n)}Q_i^{(n)}x^i=x^{\varphi(n)}Q^{(n)}\left(\frac{1}{x}\right)=\sum_{i=0}^{\varphi(n)}Q_{\varphi(n)-i}^{(n)}x^i$$

可见对 $0\leqslant i\leqslant\varphi(n)$，恒有

$$Q_i^{(n)}=Q_{\varphi(n)-i}^{(n)}$$

〈证毕〉

性质 7 的重要作用在于，一旦分圆多项式的前一半系数被确定以后，利用对称性即可得出系数的后一半，因而减少了一半工作量。

性质 8

$$Q^{(n)}(1)=\begin{cases}0, & \text{当且仅当 } n=1\\ p, & \text{当且仅当 } n \text{ 为素数 } p \text{ 之幂}\\ 1, & \text{当且仅当 } n \text{ 含两个以上素数因子。}\end{cases}$$

证明 由于条件是互不相交的，故我们只需证必要性。

(a) $$Q^{(1)}(1)=1-1=0$$

(b) 由于

$$Q^{(p^k)}(x)=Q^{(p)}(x^{p^{k-1}})$$

$$Q^{(p)}(x)=\frac{Q^{(1)}(x^p)}{Q^{(1)}(x)}=\frac{x^p-1}{x-1}=\sum_{i=0}^{p-1}x^i$$

因此

$$Q^{(p^k)}(1)=Q^{(p)}(1)=\sum_{i=0}^{p-1}1^i=p$$

(c) 设 $n=p_1^{\alpha_1}\cdots p_s^{\alpha_k}$，则有

$$Q^{(n)}(1)=Q^{(p_1\cdots p_k)}(1)=Q^{(p_1 m)}(1)$$

$$=\frac{Q^{(m)}(1^{p_1})}{Q^{(m)}(1)}=1$$

其中　$m=p_2\cdots p_k$。　　〈证毕〉

性质 9

$$Q^{(n)}(-1)=\begin{cases} 0, & \text{当且仅当 } n=2 \\ -2, & \text{当且仅当 } n=1 \\ 2, & \text{当且仅当 } n \text{ 为 2 的幂，} n \geqslant 4 \\ p, & \text{当且仅当 } n \text{ 为 } p \text{ 的幂与 2 的乘积} \\ 1, & \text{其余情形} \end{cases}$$

证明　我们只需要证明必要性。

(a) $Q^{(2)}(x)=x+1$，故$Q^{(2)}(-1)=0$

(b) $Q^{(1)}(x)=x-1$，故$Q^{(1)}(-1)=-2$

(c) $Q^{(2^k)}(x)=Q^{(2)}(x^{2^{k-1}})=x^{2^{k-1}}+1$

故$Q^{(2^k)}(-1)=1+1=2$

(d) $Q^{(2p^k)}(x)=Q^{(p^k)}(-x)$

故$Q^{(2p^k)}(-1)=Q^{(p^k)}(1)=p$

(e) 若 p 为奇素数，且 $n=p^k$，则

$$Q^{(p^k)}(-1)=Q^{(p)}((-1)^{p^{k-1}})=Q^{(p)}(-1)$$

$$=\sum_{i=1}^{p-1}(-1)^i=1$$

若 p 为奇素数，$n=pm$，且 $(p, m)=1$，则

$$Q^{(pm)}(-1)=\frac{Q^{(m)}((-1)^p)}{Q^{(m)}(-1)}=1$$

〈证毕〉

性质 8 和 9 可用于校验所求的分圆多项式的正确性。

在实际计算分圆多项式时，常利用以上诸性质简化计算过程。下面两个公式也应牢记心中：设 p 为素数，则恒有

$$Q^{(p)}(x)=\prod_{d|p}(x^d-1)^{\mu\left(\frac{p}{d}\right)}=(x-1)^{\mu(p)}(x^p-1)^{\mu(1)}$$

$$=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+x+1$$

于是

$$Q^{(p^k)}(x)=Q^{(p)}(x^{p^{k-1}})=x^{p^{k-1}(p-1)}+\cdots+x^{p^{k-1}}+1$$

例5.3.1 极易求出前几个分圆多项式

$Q^{(1)}(x)=x-1$

$Q^{(2)}(x)=x+1$

$Q^{(3)}(x)=x^2+x+1$

$Q^{(4)}(x)=x^2+1$

$Q^{(5)}(x)=x^4+x^3+x^2+x+1$

$Q^{(6)}(x)=\dfrac{Q^{(2)}(x^3)}{Q^{(2)}(x)}=\dfrac{x^3+1}{x+1}=x^2-x+1$

$Q^{(7)}(x)=x^6+x^5+x^4+x^3+x^2+x+1$

$Q^{(8)}(x)=x^4+1$

$Q^{(9)}(x)=x^6+x^3+1$

$Q^{(10)}(x)=\dfrac{Q^{(2)}(x^5)}{Q^{(2)}(x)}=\dfrac{x^5+1}{x+1}=x^4-x^3+x^2-x+1$

$Q^{(11)}(x)=x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$

$Q^{(12)}(x)=Q^{(6)}(x^2)=x^4-x^2+1$

…

注意在以上各例中，均有$\deg Q^{(n)}(x)=\varphi(n)$

当n较大时，我们往往利用性质7。这时有公式（$n\geqslant 2$）

$$Q^{(n)}(x)\equiv\prod_{d|n}\left(1-x^{\frac{n}{d}}\right)^{\mu(d)}\left(\bmod x^{\frac{\varphi(n)}{2}+1}\right)\quad(5\text{-}18)$$

我们可以利用式（5-18）计算分圆多项式的前一半系数。

例5.3.2 计算$Q^{(105)}(x)$

因为$\varphi(105)=\varphi(3\cdot5\cdot7)=2\cdot4\cdot6=48$

所以

$$Q^{(105)}(x)=\frac{(1-x^3)(1-x^5)(1-x^7)(1-x^{105})}{(1-x)(1-x^{15})(1-x^{21})(1-x^{35})}$$

$$\equiv(1+x+x^2)(1-x^5)(1-x^7)(1+x^{15})(1+x^{21})\quad(\mathrm{mod}\,x^{25})$$

在$\mathrm{mod}\,x^{25}$运算下，有

$$1-x^{105}=1\qquad 1-x^{35}=1$$

$$\frac{1}{1-x^{15}}=1+x^{15}+x^{30}+\cdots=1+x^{15}$$

$$\frac{1}{1-x^{21}}=1+x^{21}+x^{42}+\cdots=1+x^{21}$$

此外

$$(1+x+x^2)(1-x^5)(1-x^7)(1+x^{15})(1+x^{21})$$
$$=(1+x+x^2)(1-x^5-x^7+x^{12})(1+x^{15}+x^{21})$$
$$=(1+x+x^2)(1-x^5-x^7+x^{12}+x^{15}-x^{20}+x^{21}-x^{22})$$
$$=1+x+x^2-x^5-x^6-2x^7-x^8-x^9+x^{12}+x^{13}$$
$$+x^{14}+x^{15}+x^{16}+x^{17}-x^{20}-x^{22}-x^{24}$$

最后得

$$Q^{(105)}(x)=1+x+x^2-x^5-x^6-2x^7-x^8-x^9+x^{12}$$
$$+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}-x^{20}-x^{22}-x^{24}$$
$$-x^{26}-x^{28}+x^{31}+x^{32}+x^{33}+x^{34}+x^{35}+x^{38}$$
$$-x^{39}-x^{40}-2x^{41}-x^{42}-x^{43}+x^{46}+x^{47}+x^{48}$$

例5.3.3 因为

$$x^7-1=Q^{(1)}(x)Q^{(7)}(x)$$

所以

$$x^7-1=(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$$

特别在$GF(2)$上，我们进一步还有

$$(x^6+x^5+x^4+x^3+x^2+x+1)=(x^3+x+1)(x^3+x^2+1)$$

因此

$$x^7-1=(x+1)(x^3+x+1)(x^3+x^2+1)$$

这是x^7-1在$GF(2)$上的既约分解式。

一般将x^n-1的分圆分解式再进一步进行既约分解的问题，并不容易解决。以后我们将针对具体问题对于分解方法作一些说明。不仅如此，就是当n很大时，分圆多项式本身的计算也不是一件容易的事情。

§5.4 有限域的加法结构

在通常的数域中，作为单位元素的1具有这样的性质：对于任意自然数n，恒有$n\cdot 1\neq 0$。但是，在某些域中却可能发生另一种情况。例如，在$GF(2)$中，我们有$2\cdot 1=1+1=0$。在模p整数剩余类所成的域$GF(p)$中（p为素数），

$$p\cdot\bar{1}=\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{p\text{个}}=\bar{p}=\bar{0}$$

定义5.4.1 设1是域F中的单位元素。如果对于任意正整数n，恒有$n\cdot 1\neq 0$，则称域F的特征为∞(或0)。否则称满足$n\cdot 1=0$的最小正整数为域F的特征。

根据以上定义，$GF(2)$的特征为2，$GF(p)$的特征为p。

显然，若$n\cdot 1=0$，则对于任意$a\neq 0\in F$，必有$n\cdot a=0$。事实上

$$n\cdot a=\underbrace{a+\cdots+a}_{n\text{个}}=\underbrace{1\cdot a+\cdots+1\cdot a}_{n\text{个}}$$

$$=\underbrace{(1+\cdots+1)}_{n\text{个}}\cdot a=(n\cdot 1)\cdot a=0\cdot a=0$$

对于域中任意非零元素a，可以完全仿照上述定义来定义元素a的特征。

我们现在断定：域中一切非零元素的特征都是相同的，都等于域的特征。

若域F的特征为∞，则任意$a\neq 0\in F$的特征亦为∞。否

则，若存在 n，使

$$n\cdot a=(n\cdot 1)\cdot a=0$$

则因 F 中没有零因子，且 $a\neq 0$，故 $n\cdot 1=0$，矛盾。

若域 F 的特征为有限，例如 p，则任意 $a\neq 0\in F$ 的特征亦为有限。因为前面已经证明，当 $p\cdot 1=0$ 时，必有 $p\cdot a=0$。现在假定 a 的特征为 m，我们证明 $m=p$。

$$m=jp+k,\quad 0\leqslant k<p$$

从而（注意 $p\cdot 1=0$）

$$m\cdot a=(jp+k)\cdot a=jpa+ka=j(p\cdot 1)a+ka$$

$$k\cdot a=0$$

又从 $k\cdot a=0$，推出 $(k\cdot 1)\cdot a=0$，故 $k\cdot 1=0$。由于 $0\leqslant k<p$，必有 $k=0$（域的特征为 p）。由此断定，$p|m$。同理可证，$m|p$。因此 $m=p$。

综上所述，称满足 $n\cdot 1=0$ 的最小正整数为域的特征而不称为单位元素 1 的特征，就显得十分自然了。

类似于元素的阶的概念，读者不难证明特征的概念具有下述两个重要性质。

（1）若域 F 的特征为 p，则对于任何 $a\neq 0\in F$，序列

$$a,\ 2a,\ \cdots,\ (p-1)a,\ pa$$

中的元素两两互不相同。若域 F 的特征为 ∞，则对于任意 $a\neq 0\in F$，序列

$$0,\ a,\ 2a,\ \cdots,\ na,\ \cdots$$

中的元素两两互不相同。

（2）设域 F 的特征为 p，任取 $a\neq 0\in F$，则恒有

$$ma=0\ \text{当且仅当}\ p|m\ (m\ \text{为整数})$$

由上面的讨论可以看出，特征的概念体现了加法运算的循环性质，元素阶的概念体现了乘法运算的循环性质，两者都是一种周期的性质。

定理5.4.1 任意域的特征或为素数，或为 ∞。

证明 假定不然，设域的特征为

$$m = rs, \quad r, \quad s < m$$

于是

$$m \cdot 1 = (r \cdot 1)(s \cdot 1) = 0$$

但是域中没有零因子，故 $r \cdot 1 = 0$ 或 $s \cdot 1 = 0$，此与 m 为域的特征的假定矛盾。 〈证毕〉

由这一定理可以得出结论：有限域的特征必为有限。换言之，若域 F 的特征为 ∞，则 F 必为无限域。由性质（1），在特征为 ∞ 的域 F 中，序列

$$0, \ 1, \ 2 \cdot 1, \ \cdots, \ n \cdot 1, \ \cdots$$

中的元素两两互不相同，从而 F 为无限域。

但是如果域的特征为有限，则这个域可以是有限域，也可以是无限域。例如，系数取自 $GF(p)$ 的全体有理函数 $\dfrac{f(x)}{g(x)}$ 的集合就构成特征为 p 的无限域。

定义5.4.2 如果域 F 中不再含有真子集作为 F 的子域，则称 F 为素域。

定理5.4.2 在 p 特征域中，域整数（即形如 $n \cdot 1$ 的全体元素，$n = 0, \pm 1, \pm 2, \cdots$）全体构成 p 阶素子域，并且这一素子域同构于模 p 整数域 $GF(p)$。

证明 由于域的特征为 p，故域整数只有下述元素：

$$0, \ 1, \ 2 \cdot 1, \ \cdots, \ (p-1) \cdot 1$$

命 R_p 为域整数的集合，在 R_p 与 $GF(p)$ 之间建立对应

$$0 \leftrightarrow \bar{0}, \ 1 \leftrightarrow \bar{1}, \ 2 \cdot 1 \leftrightarrow \bar{2}, \ \cdots, (p-1) \cdot 1 \leftrightarrow \overline{p-1}$$

不难看出，在这一对应之下，R_p 与 $GF(p)$ 同构。因此 R_p 作为 $GF(p)$ 的同构象，自然也是 p 阶有限域。

至于 R_p 为素子域的断言是显然的，因为任何域内皆含有域整数。 〈证毕〉

更为一般的结果是

定理5.4.3 任意域 F 都含有唯一的素域作为它的素子域。当域的特征为 ∞ 时，它含有一个与有理数域同构的素子域，当域的

特征为 p 时，它含有一个与模 p 整数域 $GF(p)$ 同构的素子域。

证明 （a）当域的特征为∞时，可使有理数域与 F 的一部分元素建立下述对应：

$$\frac{q}{p} \leftrightarrow (q \cdot 1)(p \cdot 1)^{-1} = \frac{q \cdot 1}{p \cdot 1} \ (p,\ q \text{ 为正整数})$$

$$0 \leftrightarrow 0 \ (\text{域 } F \text{ 中的零元素})$$

$$-\frac{q}{p} \leftrightarrow -(q \cdot 1)(p \cdot 1)^{-1} = -\frac{q \cdot 1}{p \cdot 1}$$

这一对应是有理数域与域 F 中形如 $\pm\frac{q \cdot 1}{p \cdot 1}$ 及 0 的全体之间的同构对应。因而 F 中由 0 及形如 $\pm\frac{q \cdot 1}{p \cdot 1}$ 的元素全体构成与有理数域同构的域，它显然是 F 的素子域。

（b）当域的特征为 p 时，证法同定理5.4.2。 〈证毕〉

今后我们仍将 p 特征域中的 p 阶素子域记为 $GF(p)$。

定理5.4.4 在 p 特征域中，恒有

$$x^p - a^p = (x - a)^p \tag{5-19}$$

其中 a 为域中任一元素。

证明 由二项式定理，

$$(x - a)^p = \sum_{k=0}^{p} \binom{p}{k} (-a)^k x^{p-k}$$

当 $0 < k < p$ 时，

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

因为 $k! \mid p(p-1)\cdots(p-k+1)$，而 $(k!,\ p) = 1$，故 $k! \mid (p-1)\cdots(p-k+1)$，即 $\frac{(p-1)\cdots(p-k+1)}{k!} \triangleq n_1$ 为正整数。因此

$$\binom{p}{k}(-a)^k=(n_1p)(-a)^k=n_1(p(-a)^k)=n_1\cdot 0=0$$

注意到

$$\binom{p}{0}=\binom{p}{p}=1$$

从而

$$(x-a)^p=x^p+(-a)^p$$

当 p 为奇数时，$(-a)^p=-a^p$。当 $p=2$ 时，$(-a)^2=a^2$。但是在特征为 2 的域中，$a^2=-a^2$。因此恒有 $(-a)^p=-a^p$。

〈证毕〉

推论5.4.4.1 对于 p 特征域中的任意两个元素 a，b，恒有

$$(a\pm b)^p=a^p\pm b^p \tag{5-20}$$

证明 由定理5.4.4得

$$(x-b)^p=x^p-b^p \tag{5-21}$$

再令 $x=a$，则有

$$(a-b)^p=a^p-b^p$$

其次，在式（5-21）中令 $x=a+b$，则

$$((a+b)-b)^p=a^p=(a+b)^p-b^p$$

因而

$$(a+b)^p=a^p+b^p$$

〈证毕〉

推论5.4.4.2 在 p 特征域 F 中，任意非零元素的阶都不能是 p 的倍数。

证明 假定不然。设 $a\neq 0\in F$ 的阶为 kp，则 $a^{kp}=1$。于是

$$a^{kp}-1=(a^k-1)^p=0$$

从而 $a^k-1=0$，即 $a^k=1$，此与 a 之阶为 kp 的假定矛盾。

〈证毕〉

定理5.4.5 设 w_1，…，w_k 是 p 特征域中的元素，则对于任

意自然数 n，恒有

$$\left(\sum_{i=1}^{k} w_i\right)^{p^n} = \sum_{i=1}^{k} w_i^{p^n} \qquad (5\text{-}22)$$

证明 第一步我们证明，当 $k=2$ 时，定理对一切 n 均成立。对 n 用归纳法证明之。

当 $n=0$ 时，定理成立。今假定

$$(w_1+w_2)^{p^n}=w_1^{p^n}+w_2^{p^n}$$

于是

$$\begin{aligned}(w_1+w_2)^{p^{n+1}} &= ((w_1+w_2)^{p^n})^p \\ &= (w_1^{p^n}+w_2^{p^n})^p \text{（归纳假设）} \\ &= (w_1^{p^n})^p+(w_2^{p^n})^p \text{（推论5.4.4.1）} \\ &= w_1^{p^{n+1}}+w_2^{p^{n+1}}\end{aligned}$$

第二步我们证明，对任意固定的 n，定理对一切 k 均成立。对 k 用归纳法证明。

当 $k=2$ 时，已证定理成立。今设

$$\left(\sum_{i=1}^{k} w_i\right)^{p^n} = \sum_{i=1}^{k} w_i^{p^n}$$

于是

$$\begin{aligned}\left(\sum_{i=1}^{k+1} w_i\right)^{p^n} &= \left(\sum_{i=1}^{k} w_i + w_{k+1}\right)^{p^n} \\ &= \left(\sum_{i=1}^{k} w_i\right)^{p^n} + w_{k+1}^{p^n} \text{（第一步所得结果）} \\ &= \left(\sum_{i=1}^{k} w_i^{p^n}\right) + w_{k+1}^{p^n} \text{（归纳假设）} \\ &= \sum_{i=1}^{k+1} w_i^{p^n}\end{aligned}$$

〈证毕〉

为简便起见，在不致引起混淆的情况下，常把域整数 $k\cdot 1$

直接写成k。

推论5.4.5 1 设k为p特征域中的域整数，则对于一切自然数n，恒有

$$k^{p^n}=k \tag{5-23}$$

证明 由定理5.4.5，得

$$k^{p^n}=\left(\sum_{i=1}^{k}1\right)^{p^n}=\sum_{i=1}^{k}1^{p^n}=\sum_{i=1}^{k}1=k$$

〈证毕〉

定理5.4.6 p特征域中的元素为域整数的充分必要条件是满足方程$x^p-x=0$。

证明 因为p特征域中的全体域整数构成p阶有限域$GF(p)$，故该域中每一个元素且仅仅这些元素满足方程

$$x^p-x=0$$

〈证毕〉

大家知道，系数取自实数域的代数方程

$$f(x)=0$$

在复数域上的根是成对出现的，亦即若$a+ib$是方程$f(x)=0$的根，则$a-ib$也是方程$f(x)=0$的根。与此相当，在p特征域上我们有下面的结果。

定理5.4.7 设$f(x)$是系数取自$GF(p)$的多项式：

$$f(x)=\sum_{i=0}^{k}f_ix^i,\quad f_i\in GF(p)$$

于是，若w是方程

$$f(x)=0$$

的根，则对于一切自然数n，w^{p^n}也是该方程的根。

证明 由假设

$$f(w)=\sum_{i=0}^{k}f_iw^i=0$$

于是由定理5.4.5得

$$0=(f(w))^{p^n}=\left(\sum_{i=0}^{k} f_i w^i\right)^{p^n}=\sum_{i=0}^{k} f_i^{p^n} w^{ip^n}$$

$$=\sum_{i=0}^{k} f_i^{p^n}(w^{p^n})^i$$

因为f_i为域整数，故由推论5.4.5.1，$f_i^{p^n}=f_i$。所以

$$0=\sum_{i=0}^{k} f_i^{p^n}(w^{p^n})^i=\sum_{i=0}^{k} f_i(w^{p^n})^i=f(w^{p^n})$$

〈证毕〉

注意多项式 $f(x)$ 的次数是有限的。因此，方程 $f(x)=0$ 在任意域上根的数目总是有限的。这表明在序列

$$w,\ w^p,\ w^{p^2},\ \cdots,\ w^{p^n},\ \cdots$$

中必有重复的元素，而其中实质上不同的元素只能是有限个。于是若 p 特征域中的一个非零元素 w 是系数取自域整数上的某一代数方程的根，则 w 必为有限阶元素。

§5.5 最小多项式与本原多项式

当 w 为 p 特征有限域中的一个 n 阶元素时，序列

$$w,\ w^p,\ w^{p^2},\ \cdots,\ w^{p^n},\ \cdots \tag{5-24}$$

是由元素 w 所生成的循环群

$$\langle w\rangle=\{1,\ w,\ w^2,\ \cdots,\ w^{n-1}\}$$

的一个子集。因此，序列（5-24）中真正不同的元素的个数必然与元素 w 的阶有密切关系。下述定理就指出了这种精确的关系。

定理5.5.1 如果 w 是 p 特征有限域上的 n 阶元素，而 m 是 p 关于模 n 的阶❶，则必有

$$w^{p^m}=w$$

并且 m 个元素

$$w,\ w^p,\ w^{p^2},\ \cdots,\ w^{p^{m-1}} \tag{5-25}$$

---

❶ 回忆 m 是满足 $p^m\equiv 1\pmod{n}$ 的最小正整数，其中 $(p,n)=1$。由推论5.4.4.2，$p\nmid n$，从而 $(p,n)=1$。因此，p 的模 n 阶是有意义的。

彼此不同。

证明 设 i，k 为整数，且 $0\leqslant i<k\leqslant m$，则我们有下面一系列等价关系：

$$w^{p^k}=w^{p^i}\Longleftrightarrow w^{p^k-p^i}=1\Longleftrightarrow n\,|\,p^k-p^i$$

$$\Longleftrightarrow p^k\equiv p^i \pmod n$$

$$\Longleftrightarrow p^{k-i}\equiv 1 \pmod n \text{（定理3.2.6，此处 } (p^i, n)=1\text{）}$$

$$\Longleftrightarrow m\,|\,(k-i)$$

由此得出以下结果。

（1）取 $i=0$，$k=m$，则因 $m|m$，故有

$$w^{p^m}=w$$

（2）若序列（5-25）中有两个元素相同，比如

$$w^{p^k}=w^{p^i}$$

不妨设 $k>i$，则由上面的推证，必有 $m|(k-i)$。但是 $0\leqslant i<k<m$，故 $0<k-i<m$，从而 $m\nmid(k-i)$，产生矛盾。 〈证毕〉

设 w 是 p 特征有限域上的 n 阶元素，则 w 是系数取自 $GF(p)$ 上的多项式 x^n-1 的根。系数取自 $GF(p)$ 上且以 w 为根的全体首一多项式中必有一个次数最低者。我们称这个以 w 为根且次数最低的 $GF(p)$ 上的首一多项式为 w **的最小多项式**，通常记为 $m(x)$。

定理5.5.2 在 p 特征有限域中，任意元素都有一个唯一的最小多项式 $m(x)$。此外，$m(x)$ 在 $GF(p)$ 上是既约多项式，且整除 $GF(p)$ 上任意以 w 为根的多项式。

证明 设 w 是 p 特征有限域中的任一元素，则它的最小多项式 $m(x)$ 一定是既约的。否则，设 $m(x)=r(x)s(x)$，其中 $\deg r<\deg m$，$\deg s<\deg m$，则由 $m(w)=0$ 可推出 $r(w)=0$ 或 $s(w)=0$，此与 $m(x)$ 的定义矛盾。

设 $f(x)$ 是 $GF(p)$ 上的多项式，且 $f(w)=0$，则有

$f(x)=m(x)q(x)+r(x)$　$\deg r<\deg m$ 或 $r(x)=0$。将 $x=w$ 代入上式，得 $r(w)=0$，因此 $r(x)=0$ 即 $m(x)|f(x)$。

设$m_1(x)$ 为 w 的另一个最小多项式，则因 $m_1(x)|m(x)$，$m(x)|m_1(x)$，故以上两个首一多项式相等。这就证明了最小多项式的唯一性。〈证毕〉

定理5.5.3　设 w 是 p 特征有限域中的 n 阶元素，而 m 是 p 的模 n 阶，则 w 的最小多项式 $m(x)$ 亦为 m 次多项式，并且

$$m(x)=\prod_{i=0}^{m-1}(x-w^{p^i})$$

证明　记

$$f(x)\triangleq\prod_{i=0}^{m-1}(x-w^{p^i})=\prod_{i=0}^{m}f_ix^i$$

我们先证明，$f(x)$ 是$GF(p)$ 上的多项式。由定理5.4.4，并且注意到$w^{p^m}=w^{p^0}=w$ 则有

$$(f(x))^p=\prod_{i=0}^{m-1}(x-w^{p^i})^p=\prod_{i=0}^{m-1}(x^p-w^{p^{i+1}})$$

$$=\prod_{i=1}^{m}(x^p-w^{p^i})=\prod_{i=0}^{m-1}(x^p-w^{p^i})=f(x^p)$$

另一方面

$$(f(x))^p=\left(\sum_{i=0}^{m}f_ix^i\right)^p=\sum_{i=0}^{m}f_i^px^{pi}$$

$$f(x^p)=\sum_{i=0}^{m}f_ix^{pi}$$

因此对于任意 i ($i=0, 1, \cdots, m$)，恒有

$$f_i^p=f_i$$

根据定理5.4.6，$f_i\in GF(p)$。

其次由定理5.4.7，任意$GF(p)$上的多项式若以w为根，则必以全体元素

$$w,\ w^{p},\ w^{p^2},\ \cdots,\ w^{p^{m-1}}$$

为根。因此m次多项式

$$f(x)=\sum_{i=0}^{m-1}(x-w^{p^i})$$

为$GF(p)$上以w为根且次数最低的首一多项式。于是$m(x)=f(x)$。 〈证毕〉

元素w的最小多项式的次数称为**域元素w的次数**。

由上述讨论可见，域元素w的次数等于p的模n阶，其中p为域的特征，n为元素w的阶。

显而易见，元素w^p，w^{p^2}，…，$w^{p^{m-1}}$必与元素w有相同的阶，从而它们有相同的最小多项式。在这个意义上，我们称序列

$$w,\ w^{p},\ \cdots,\ w^{p^{m-1}}$$

为**共轭元素**系。

这正如在复数域中把$\pm i$叫作共轭复数一样，因为它们都是系数在实数域上的多项式Z^2+1的根。

不难看出，域元素w的最小多项式实际上就是以w为根的$GF(p)$上既约的首一多项式。

定义5.5.1 q阶有限域中本原域元素的最小多项式叫作**本原多项式**。

本原多项式的概念在编码理论中至为重要，请读者予以充分重视。

定理5.5.4 设w是p特征有限域中的m次域元素，则$GF(p)$上次数$<m$的w的多项式全体F构成p^m阶子域。

证明 我们分四步证明。

（1）F中的多项式两两互不相同。若F中有两个多项式相同

$$\sum_{i=0}^{m-1} a_i w^i = \sum_{i=0}^{m-1} a'_i w^i,\ a_i,\ a'_i \in GF(p),$$

其中a_i与a'_i不全相同($i=0, 1, \cdots, m-1$)，则

$$\sum_{i=0}^{m-1} (a_i - a'_i) w^i = 0$$

这表明$GF(p)$上的非零多项式

$$f(x) \triangleq \sum_{i=0}^{m-1} (a_i - a'_i) w^i$$

以w为根，且$\deg f(x) < m$，此与w为m次域元素的假定矛盾。因此F中共有p^m个多项式。

(2) 证明F为原来的p特征有限域（作为环看待）中的一个交换子环。

设$f(w)$，$g(w) \in F$，显然$f(w) - g(w) \in F$。其次设$h(x) = f(x)g(x)$，且设$m(x)$为w的最小多项式。由欧几里德除法，

$h(x) = m(x)q(x) + r(x)$，$\deg r < \deg m$，或$r(x) = 0$。从而$h(w) = m(w)q(w) + r(w) = r(w)$。因为$r(w) \in F$，故$h(w) = f(w)g(w) \in F$。于是，$F$构成交换子环。

(3) F含有单位元素。事实上，原来域中的单位元素即为F的单位元素。

(4) 证明F中的任意非零元素都有逆元素。

设$g(w) \neq 0 \in F$，且$m(x)$为w的最小多项式。由于$(m(x), g(x)) = 1$，故存在$a(x)$，$b(x) \in GF(p)[x]$，使

$$a(x)g(x) + b(x)m(x) = 1$$

由定理3.1.4得

$$\deg a(x) < m,\ \deg b(x) < m$$

因此

$$a(w)g(w) + b(w)m(w) = a(w)g(w) = 1$$

亦即$a(w)\in F$是$g(w)$的逆元素。

综上所述，F构成p^m阶子域。 《证毕》

§5.6 有限域的代数结构

在前面几节里，我们分别针对有限域的乘法与加法运算讨论了它们的结构。在这一基础上，我们现在讨论有限域的代数结构。

定理5.6.1 有限域的阶必为其特征（素数）之幂。

证明 假定域的阶为q，特征为p。设α为该域中的一个$q-1$阶本原元，又设m为p的模$q-1$阶，则

$$\alpha^{p^m}=\alpha，\text{或}\alpha^{p^m-1}=1$$

由此断定$(q-1)|(p^m-1)$。因此，$q-1\leqslant p^m-1$，或$q\leqslant p^m$。

另一方面，由于α是m次域元素，则根据定理5.5.4，系数取自$GF(p)$且次数低于m的全体α的多项式构成这个q阶有限域的p^m阶子域。因此，$p^m\leqslant q$。 《证毕》

由这一定理可以断定，有限域中所含元素的个数必为某一个素数之幂。并且q阶有限域共含p^m个元素，其中p为该有限域的特征，m为p关于模$q-1$的阶。

定理5.6.2 设$f(x)$为q阶有限域F上的一个d次既约多项式，则多项式剩余类集合$F[x]\mathrm{mod}\,f(x)$构成q^d阶有限域$\bar{F}$，$\bar{F}$是域F的扩域，并且$f(x)$在$\bar{F}$内有根。

证明 定理的三个部分证明如下：

(1) 由定理3.6.3，$F[x]\mathrm{mod}f(x)$构成域，它显然是阶为q^d的有限域。

(2) 证明$\bar{F}$为F的扩域（在同构的意义下）。

对于$a\in F$，令它对应$\bar{F}$中的$\overline{a+0\cdot x+\cdots+0\cdot x^{d-1}}=\bar{a}$，即

$$a\leftrightarrow\bar{a},$$

这是F与$\bar{F}$的一个子集$\bar{F}'=\{\bar{a}\in\bar{F}\}$之间的一一对应，并且当$a$

$\leftrightarrow \bar{a}$, $b \leftrightarrow \bar{b}$时，显然

$$a+b \leftrightarrow \bar{a}+\bar{b}, \quad a \cdot b \leftrightarrow \bar{a} \cdot \bar{b}$$

因此，这一对应是F与$\bar{F}'$之间的同构对应。由于F是域，故$\bar{F}'$也是域。如果将F与$\bar{F}'$视为同一，而$\bar{F}$是$\bar{F}'$的扩域，则$\bar{F}$也是F的扩域（参见图5-2)。

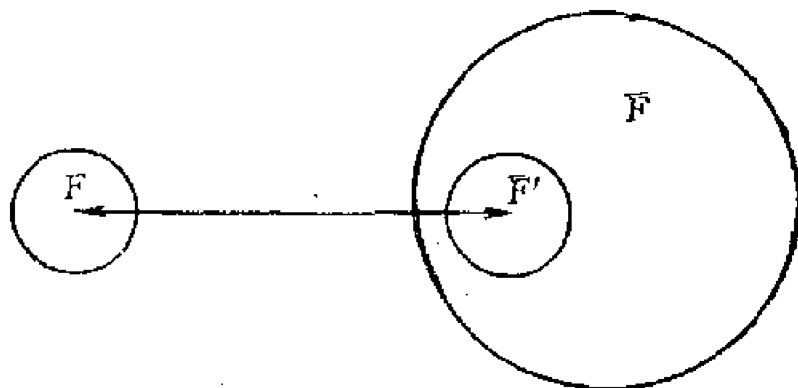

图 5-2

（3）设$\alpha=\bar{x}$，且设

$$f(x)=f_0+f_1x+\cdots+f_dx^d$$

则

$$f(\alpha)=f(\bar{x})=f_0+f_1\bar{x}+\cdots+f_d\bar{x}^d$$
$$=\overline{f_0+f_1x+\cdots+f_dx^d}=\bar{f}(x)=\bar{0}$$

这表明$\alpha=\bar{x}$是$f(x)$的根。 〈证毕〉

前面所讲过的最小多项式的概念可以推广到一般情形。设F是一个域，而E是F的一个扩域。若$\alpha\in E$，则系数取自F，且以α为根的次数最低的首一多项式称为α（关于域F）的最小多项式。这里应当注意的是，与有限域的情形不同，并非扩域E中的每一个元素α都有最小多项式。用类似于定理5.5.2的方法可以证明，如果存在扩域E中元素α的最小多项式，则一定是唯一的，它是域F上的既约多项式，并且整除任意系数取自F且以α为根的多项式。由此可见，E中元素α的最小多项式实际上就是以α为根的域F上的首一既约多项式。

定理5.6.3 设n是任意正整数，则q阶有限域中的任意元

素都满足方程

$$x^{q^n} - x = 0$$

证明 用归纳法证明。当 $n = 1$ 时，由定理5.1.1，结论成立。今假定结论对 $n - 1$ 成立，即该 q 阶域中的任意元素皆满足方程

$$x^{q^{n-1}} - x = 0$$

于是，对于任意域元素 α 恒有

$$\alpha^{q^n} = (\alpha^{q^{n-1}})^q = \alpha^q = \alpha$$

〈证毕〉

定理5.6.4 设 $f(x)$ 是 q 阶有限域上的一个 d 次既约多项式。于是，若 $d|k$，则

$$f(x)|x^{q^k} - x$$

证明 令 $k = dn$。由定理5.6.2，模 $f(x)$ 的剩余类集合构成q^d阶有限域，且 $f(x)$ 在该域中有根 α。再由定理5.6.3，这个q^d阶域中的任意元素均满足方程

$$x^{(q^d)^n} - x = x^{q^{dn}} - x = x^{q^k} - x = 0$$

由此可得，$\alpha^{q^k} - \alpha = 0$。这表明 α 同时是 $f(x)$ 及 $x^{q^k} - x$ 的根。我们知道，q^d 阶域中元素 α 的最小多项式即为 $f(x)$（当 $f(x)$ 不是首一多项式时，至多相差一个常数因子）。因此，$f(x)|x^{q^k} - x$。 〈证毕〉

例5.6.1 考虑多项式$x^8 + x$ 在$GF(2)$ 上的分解。

由定理5.6.4，$GF(2)$ 上每一个 1 次多项式和 3 次既约多项式均能整除$x^{2^3} + x = x^8 + x$。$GF(2)$ 上次数为 1、3的全部既约多项式的乘积为

$$x(x+1)(x^3+x+1)(x^3+x^2+1)$$

它必能整除$x^8 + x$。由于这一乘积是 8 次首一多项式，故必有

$$x^8 + x = x(x+1)(x^3+x+1)(x^3+x^2+1)$$

上式亦不难通过实际计算予以证实。

受这个例子的启发，我们有

定理5.6.5 在 q 阶有限域中，$x^{q^k} - x$ 可以分解为次数整除

k 的所有 q 阶域上相异首一既约多项式的乘积。

在证明这一定理之前，我们需要一个引理.

引理5.6.1 设 k，m，n 为正整数，且 $k\geqslant 2$，$m\geqslant 1$，$n\geqslant 1$，则

$$(k^m-1)|(k^n-1)\ \text{当且仅当}\ m|n$$

证明 由欧几里德除法，

$$n=qm+r,\quad 0\leqslant r<m$$

于是

$$\frac{k^n-1}{k^m-1}=\frac{k^r(k^{qm}-1)}{k^m-1}+\frac{k^r-1}{k^m-1}$$

我们知道，$(k^m-1)|(k^{qm}-1)$，且 $\frac{k^r-1}{k^m-1}<1$。

因此，$(k^m-1)|(k^n-1)$ 当且仅当 $\frac{k^r-1}{k^m-1}$ 为整数，

当且仅当 $r=0$，当且仅当 $m|n$。〈证毕〉

定理5.6.5的证明 由定理5.6.4，若 $f(x)$ 为 q 阶有限域上的首一 d 次既约多项式，且 $d|k$，则 $f(x)|(x^{q^k}-x)$。

剩下来只需证明，若 $f(x)$ 为 q 阶有限域 F 上的首一 d 次既约多项式，且 $f(x)|(x^{q^k}-x)$，则 $d|k$。

由定理5.6.2，模 $f(x)$ 的剩余类集合构成 q^d 阶有限域 $\bar{F}$，且 $f(x)$ 在 $\bar{F}$ 中有根 α。于是我们可以将 $\bar{F}$ 中的任意元素，例如本原元 β，表示成系数取自 F 且次数低于 d 的 α 的多项式

$$\beta=a_0+a_1\alpha+\cdots+a_{d-1}\alpha^{d-1}$$

其中 a_0，a_1，…，$a_{d-1}\in F$。

由于 $f(\alpha)=0$，故 $\alpha^{q^k}=\alpha$。根据定理5.4.5，5.6.1及推论5.4.5.1，我们有

$$\begin{aligned}\beta^{q^k}&=(a_0+a_1\alpha+\cdots+a_{d-1}\alpha^{d-1})^{q^k}\\&=a_0^{q^k}+a_1^{q^k}\alpha^{q^k}+\cdots+a_{d-1}^{q^k}\alpha^{(d-1)q^k}\\&=a_0+a_1\alpha+\cdots+a_{d-1}\alpha^{d-1}\\&=\beta\end{aligned}$$

于是$\beta^{q^k-1}=1$。但是β是q^d-1阶元素，故$q^d-1|q^k-1$。由引理5.6.1，$d|k$。

〈证毕〉

定理5.6.6 设$f(x)$为$GF(p)$上的m次既约多项式，且$m|k$，则任何p^k阶有限域必含有$f(x)$的全部（m个）根。

证明 由定理5.6.5，在$GF(p)$上，

$$x^{p^k}-x=\prod_{\deg g(x)|k} g(x) \quad (g(x)\text{为}GF(p)\text{上首一既约多项式})。$$

另一方面，在p^k阶域中，$x^{p^k}-x$可以分解为p^k个一次因式

$$x^{p^k}-x=\prod_{\alpha\in p^k\text{阶域}}(x-\alpha)$$

在p^k阶域中，这两种分解应当相等（从同构的观点，$GF(p)$是一切p特征域的子域）

$$\prod_{\deg g(x)|k} g(x)=\prod_{\alpha\in p^k\text{阶域}}(x-\alpha)$$

由于m次既约多项式$f(x)$是上述等式左边的一个因式，故可在等式右边挑出属于$f(x)$的全部m个一次因式，即

$$f(x)=\prod_{j=1}^{m}(x-\alpha_{i_j})$$

〈证毕〉

注意定理中p改为q，该定理显然也成立。

我们已经知道，任意有限域的阶皆为某一素数p之幂p^m。反过来对于任意素数p和正整数m，一定可以找到一个p^m阶的有限域。事实上，任取一个$GF(p)$上的m次既约多项式（其存在性的证明参看下面的推论5.7.1.1），由定理5.6.2，$GF(p)[x]\bmod f(x)$即构成p^m阶有限域。并且对于给定的p和m，在同构的意义上，这种p^m阶的有限域还是唯一的。由定理5.6.6，阶为p^m的任何有限域必包含$GF(p)$上m次既约多项式$f(x)$

的全部根。若令 $f(x)$ 的一个根为 α，则可将该 p^m 阶域中的任意元素表示成系数取自 $GF(p)$ 且次数低于 m 的 α 的多项式。显然在任何 p^m 阶域上，这种多项式的全体是彼此同构的。因此我们得到了关于有限域代数结构的一个重要定理。

定理5.6.7 任意有限域的阶都是一个素数的幂 p^m。反过来对于任意素数 p 和正整数 m，必存在唯一的（在同构的意义上）p^m 阶有限域。

今后凡 p^m阶有限域一律不加区别，并且统一地记成$GF(p^m)$。

从工程实践的观点来看，过分强调有限域的唯一性并无益处。根据电路设计的经济价值及其他一些因素，我们可以选择有限域的任何一种表示来适应具体的要求。

最后我们给出一个关于子域的充分必要条件。

定理5.6.8 $GF(q^k)$ 是 $GF(q^j)$ 的子域当且仅当 $k|j$。

证明 很明显地，次数整除 k 的首一既约多项式的集合是次数整除 j 的首一既约多项式集合的子集，当且仅当 $k|j$。由定理 5.6.5，并且 $GF(q^k)$ 中的q^k 个元素是方程 $x^{q^k}-x=0$ 的全部根，因此当 q 为某个素数之幂时，即得本定理。

若 $f(x)$ 为 $GF(q)$ 上的 m 次既约多项式，则 $f(x)$ 的每一个根都属于 $GF(q^m)$。设 w 是 $f(x)$ 的一个根，则 $f(x)$ 的全部根为 w，w^q，w^{q^2}，$\cdots w^{q^{m-1}}$。我们称它们为 q—共轭元素系。一般地，若 q 为某个素数 p 之幂，则 q—共轭元素系是以前所说的 p—共轭元素系的一个子集。

§5.7 既约多项式的计数

设 $I_q(k)$ 表示 $GF(q)$ 上 k 次首一既约多项式的个数。由定理 5.6.5，$GF(q)$ 上所有相异的次数整除 k 的首一既约多项式的次数之和应当等于 q^k，即

$$q^k=\sum_{d|k} dI_q(d)$$

根据麦比乌斯反转公式，立得

定理5.7.1

$$I_q(k)=\frac{1}{k}\sum_{d\mid k}\mu(d)\,q^{\frac{k}{d}}$$

上式即称为 $GF(q)$ 上 k 次首一既约多项式的计数公式。

例5.7.1 在 $GF(2)$ 上，我们有

$$I_2(1)=\mu(1)\cdot 2=2$$

$$I_2(2)=\frac{1}{2}(\mu(1)\cdot 2^2+\mu(2)\cdot 2)=\frac{1}{2}(4-2)=1$$

$$I_2(3)=\frac{1}{3}(\mu(1)\cdot 2^3+\mu(3)\cdot 2)=\frac{1}{3}(8-2)=2$$

$$I_2(4)=\frac{1}{4}(\mu(1)\cdot 2^4+\mu(2)\cdot 2^2+\mu(4)\cdot 2)$$

$$=\frac{1}{4}(16-4)=3$$

$$I_2(5)=\frac{1}{5}(\mu(1)\cdot 2^5+\mu(5)\cdot 2)=\frac{1}{5}(32-2)=6$$

等等。

例5.7.2 在 $GF(3)$ 上，我们有

$$I_3(1)=\mu(1)\cdot 3=3$$

$$I_3(2)=\frac{1}{2}(\mu(1)\cdot 3^2+\mu(2)\cdot 3)=\frac{1}{2}(9-3)=3$$

$$I_3(3)=\frac{1}{3}(\mu(1)\cdot 3^3+\mu(3)\cdot 3)=\frac{1}{3}(27-3)=8$$

$$I_3(4)=\frac{1}{4}(\mu(1)\cdot 3^4+\mu(2)\cdot 3^2+\mu(4)\cdot 3)$$

$$=\frac{1}{4}(81-9)=18$$

$$I_3(5)=\frac{1}{5}(\mu(1)\cdot 3^5+\mu(5)\cdot 3)=\frac{1}{5}(243-3)=48$$

等等。

推论5.7.1.1 对于任意 $q(=p^m)$ 与 k（k 为正整数），恒有

$$I_q(k)\geqslant 1$$

证明 由于$\mu(d)\geqslant -1$，故在定理5.7.1中，对$d>1$以-1代替$\mu(d)$就得到$I_q(k)$的一个下界：

$$I_q(k)>(q^k-q^{k-1}-\cdots-1)/k=\frac{q^k(q-2)+1}{(q-1)k}>0$$

《证毕》

这个推论在证明有限域的代数结构定理（定理5.6.7）时曾起过重要作用。

定理5.6.5不但能推出既约多项式的计数公式，还可以用来求出既约多项式。

例如在$GF(2)$上，当$k=1$时，由

$$x^2+x=x(x+1)$$

可知，共有2个1次既约多项式，即x和$x+1$。当$k=2$时，由

$$x^{2^2}+x=x^4+x=x(x+1)(x^2+x+1)$$

可知，仅有1个2次既约多项式 x^2+x+1。

又如在$GF(3)$上，当$k=1$时有

$$x^3-x=x(x-1)(x+1)$$

因此共有3个1次首一既约多项式，即x，$x-1$和$x+1$。当$k=2$时有

$$\begin{aligned}x^{3^2}-x&=x(x^8-1)=x(x-1)(x+1)\\&\quad(x^2+1)(x^4+1)=x(x-1)(x+1)\\&\quad(x^2+1)(x^2+x+2)(x^2+2x+2)\end{aligned}$$

所以共有3个2次首一既约多项式，即x^2+1，x^2+x+2和x^2+2x+2。注意还有3个2次非首一既约多项式是$2x^2+2$，$2x^2+2x+1$和$2x^2+x+1$。

§5.8 例

在这一节中，我们用一个能充分反映有限域特点的例子，即$GF(16)$，来总结一下前面所讲的关于有限域的基本理论，同时也借此进一步熟悉有限域中的代数运算方法。

我们主要讨论$GF(2)$和$GF(16)$上$x^{16}-x$的因式分解问

题，以及$GF(16)$的几种表示方法。

大家知道，$GF(16)$的全部元素的集合恰好是方程$x^{16}-x=0$的根的集合。为此，我们先以$x^{16}-x$的分圆分解入手

$$x^{16}-x=x(x^{15}-1)=x\prod_{d|15}Q^{(d)}(x)$$
$$=xQ^{(1)}(x)Q^{(3)}(x)Q^{(5)}(x)Q^{(15)}(x)$$

由例5.3.1，我们有

$$Q^{(1)}(x)=x-1$$
$$Q^{(3)}(x)=x^2+x+1$$
$$Q^{(5)}(x)=x^4+x^3+x^2+x+1$$

现在计算$Q^{(15)}(x)$如下：

$$Q^{(15)}(x)=\frac{Q^{(3)}(x^5)}{Q^{(3)}(x)}=\frac{x^{10}+x^5+1}{x^2+x+1}$$
$$=x^8-x^7+x^5-x^4+x^3-x+1$$

注意上述分圆分解对任意域都成立。但我们现在讨论的是特征为2的域，因此可将"－"号一律改成"＋"号。

我们已经知道，x，$x+1$和x^2+x+1是$GF(2)$上的既约多项式。对于$Q^{(5)}(x)=x^4+x^3+x^2+x+1$，因为2的模5阶为4，故5阶域元素的最小多项式是4次多项式，因此$Q^{(5)}(x)$是$GF(2)$上的既约多项式。但是对于$Q^{(15)}(x)$，由于2的模15阶为4，而$Q^{(15)}(x)$为8次多项式，故可分解为两个$GF(2)$上的4次既约多项式。因为多项式$Q^{(15)}(x)$的根是$GF(16)$的本原域元素，故这两个4次既约多项式实际上是$GF(16)$的本原多项式。

下面我们用两种方法对$Q^{(15)}(x)$进行既约分解。

一种是待定系数法。

$Q^{(15)}(x)$的既约因式必定形如

$$x^4+Ax^3+Bx^2+Cx+1$$

其中常数项为1，其原因是$Q^{(15)}(x)$中不含因式x。此外A，B，$C\in GF(2)$，并且

$$A+B+C=1$$

这是因为1不是15阶元素，故1不是该多项式的根。因此或者$A=B=C=1$，或者A，B，C中只有一个为1。前者导致$Q^{(5)}(x)=x^4+x^3+x^2+x+1$，这不可能。于是$A$，$B$，$C$中有一个且仅有一个为1。当$B=1$，$A=C=0$时，

$$x^4+Ax^3+Bx^2+Cx+1=x^4+x^2+1=(x^2+x+1)^2$$

当$A=1$，$B=C=0$；$C=1$，$A=B=0$时，就得到了两个4次既约多项式x^4+x^3+1和x^4+x+1。所以

$$Q^{(15)}(x)=(x^4+x^3+1)(x^4+x+1)$$

顺便指出，由例5.7.1知，$I_2(4)=3$。我们已经求出$GF(2)$上的3个4次既约多项式，它们是x^4+x+1，x^4+x^3+1和$x^4+x^3+x^2+x+1$；只有前两个是本原多项式。

另一种是变换法。

引理5.8.1 若$u\in GF(q)$，$w\in GF(q^m)$，则变换$w\to w+u$将共轭元素系仍变为共轭元素系，并且变换$x\to x+u$将既约多项式仍变为既约多项式。

证明 留作习题。

应用这个引理对$Q^{(15)}(x)$进行既约分解。已知$Q^{(5)}(x)=x^4+x^3+x^2+x+1$是既约多项式，故

$$Q^{(5)}(x+1)=(x+1)^4+(x+1)^3+(x+1)^2+(x+1)+1=x^4+x^3+1$$

亦为既约多项式。由定理5.6.5

$$x^{2^4}-x=xQ^{(1)}(x)Q^{(3)}(x)Q^{(5)}(x)Q^{(15)}(x)$$

必可分解为次数整除4的一切相异首一既约多项式的乘积。但是x^4+x^3+1不能整除x，$Q^{(1)}(x)$，$Q^{(3)}(x)$和$Q^{(5)}(x)$，故必有

$$x^4+x^3+1\,|\,Q^{(15)}(x)$$

$Q^{(15)}(x)$的另一个既约因式可以通过x^4+x^3+1除$Q^{(15)}(x)$而得到。更简单的方法则需要利用互反多项式的性质。

定理5.8.1 互反多项式有如下性质：

（1）$\tilde{\tilde{f}}(x)=f(x)$

（2）设 $f(x)=a(x)b(x)$，则 $\tilde{f}(x)=\tilde{a}(x)\tilde{b}(x)$

（3）$f(x)$ 为既约多项式，当且仅当$\tilde{f}(x)$为既约多项式

（4）$f(\alpha)=0$，当且仅当$\tilde{f}\left(\frac{1}{\alpha}\right)=0$

（5）$f(x)$ 为本原多项式，当且仅当 $\tilde{f}(x)$ 为本原多项式

证明

（1）显然。这一性质表明，$f(x)$ 和$\tilde{f}(x)$ 互为互反多项式。这就是互反多项式名称的来源。

（2）设

$$a(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$$

$$b(x)=b_0+b_1x+\cdots+b_{m-1}x^{m-1}+b_mx^m$$

其中 $a_0a_n\neq 0$，$b_0b_m\neq 0$

于是

$$f(x)=a(x)b(x)=\sum_{s=0}^{m+n}\left(\sum_{i+j=s}a_ib_j\right)x^s$$

$$\tilde{a}(x)\tilde{b}(x)=\sum_{s=0}^{m+n}\left(\sum_{i+j=n+m-s}a_ib_j\right)x^s=\tilde{f}(x)$$

这一性质可推广到 n 个多项式相乘的情形，在实际计算中很有用处。

（3）由（2）即得。

（4）若 $f(\alpha)=0$，则$\tilde{f}\left(\frac{1}{\alpha}\right)=\alpha^{-\deg f(x)}f(\alpha)=0$

反之亦然。这一性质表明，α 是 $f(x)$的根当且仅当α^{-1}是 $\tilde{f}(x)$ 的根。

（5）因为 α 和α^{-1}有相同的阶，故 α 是本原域元素当且仅当α^{-1}是本原域元素。

（证毕）

根据上述定理，x^4+x^3+1 的互反多项式

$$x^4(x^{-4}+x^{-3}+1)=x^4+x+1$$

亦为既约多项式。若 α 为 x^4+x^3+1 在 $GF(16)$ 的根，则 α^{-1} 是 x^4+x+1 的根。由于 α 为 15 阶元素，故 α^{-1} 也是 15 阶元素，因此

$$(x^4+x+1)|Q^{(15)}(x)$$

由此得

$$Q^{(15)}(x)=(x^4+x^3+1)(x^4+x+1)$$

不论采取哪一种方法，我们都得到了 $x^{16}-x$ 在 $GF(2)$ 上的既约分解

$$\begin{aligned}x^{16}-x=x(x+1)(x^2+x+1)\\(x^4+x^3+x^2+x+1)(x^4+x^3+1)\\(x^4+x+1)\end{aligned}$$

下面我们考虑 $x^{16}-x$ 在 $GF(16)$ 上的一次因式分解问题。

由定理 5.6.6，$GF(2)$ 上的 2 次既约多项式应在 $GF(2^2)=GF(4)$ 上完全分解为一次因式：

$$x^2+x+1=(x+\xi)(x+\partial)$$

根据根与系数的关系，得

$$\xi+\partial=1,\ \xi\partial=1$$

由定理 5.6.5，$x^{16}-x=x^{4^2}-x$ 可以分解为 $GF(4)$ 上次数整除 2 的所有首一既约多项式的乘积：

$$\begin{aligned}x^{16}-x=x(x+1)(x+\xi)(x+\partial)(x^2+\xi x+1)\\\cdot(x^2+\partial x+1)(x^2+\xi x+\xi)(x^2+\partial x+\partial)\\(x^2+x+\xi)(x^2+x+\partial)\end{aligned}$$

请读者注意，这里的共轭根 ξ 和 ∂ 是成对出现的，正如在实多项式分解因式时，复共轭根成对出现一样。例如，共轭虚数 i 和 $-i$ 为同一个实系数 2 次既约多项式的根，即

$$x^2+1=(x+i)(x-i)$$

与此完全相同，当 $x^2+\xi x+1$ 是 $x^4+x^3+x^2+x+1$ 的因式时，$x^2+\partial x+1$ 亦为该多项式的因式。事实上

$$
\begin{aligned}
(x^2+\xi x+1)(x^2+\partial x+1)&=x^4+(\xi+\partial)x^3\\
&\quad+(1+\xi\partial+1)x^2+(\xi+\partial)x+1\\
&=x^4+x^3+x^2+x+1
\end{aligned}
$$

其余情形也是类似的。至于上述分解中的 6 个$GF(4)$上的 2 次多项式的既约性，可以通过直接验证来判断。例如，对于$x^2+\xi x+1$，显然$GF(4)$中的 4 个元素 0，1，ξ和∂都不是它的根，因而它在$GF(4)$上是既约的。

为进一步将$x^{16}-x$完全分解为一次因式，我们必须将$GF(4)$再扩充为$GF(4^2)=GF(16)$。这样一来，$GF(4)$上的 2 次既约多项式在$GF(4^2)$中就可以完全分解为一次因式的乘积。

从$GF(4)$扩充到$GF(16)$，需增加 12 个元素，我们分别用希腊字母表示它们。因而有

$$
\begin{array}{lllll}
x^{16}-x= & xQ^{(1)}(x) & Q^{(3)}(x) & Q^{(5)}(x) & Q^{(15)}(x)\\
= & x(x+1) & (x^2+x+1) & (x^4+x^3+x^2+x+1) & (x^8+x^7+x^5+x^4\\
 & & & & +x^3+x+1)\\
= & x(x+1) & (x^2+x+1) & (x^4+x^3+x^2+x+1) & (x^4+x^3+1)\\
 & & & & (x^4+x+1)\\
= & x(x+1) & (x+\xi)(x+\partial) & (x^2+\xi x+1) & (x^2+\xi x+\xi)\\
 & & & (x^2+\partial x+1) & (x^2+x+\xi)\\
 & & & & (x^2+\partial x+\partial)\\
 & & & & (x^2+x+\partial)\\
= & x(x+1) & (x+\xi)(x+\partial) & (x+\delta)(x+\mu) & (x+\beta)(x+\theta)\\
 & & & (x+\gamma)(x+\theta) & (x+\alpha)(x+\pi)\\
 & & & & (x+\lambda)(x+\zeta)\\
 & & & & (x+\varphi)(x+\rho)
\end{array}
$$

最后我们讨论$GF(16)$的几种表示方法。

第一种是通过本原域元素的幂表示$GF(16)$。

设α是$GF(16)$的一个本原域元素。为明确起见，不妨设α为方程$x^2+x+\xi=0$的根。于是$GF(16)$的全部元素都可以用序列

$$0,\ 1=\alpha^0,\ \alpha^1,\ \alpha^2,\ \cdots,\ \alpha^{14},\ \alpha^{15}$$

表示。

我们可以通过α的幂来分辨出$GF(16)$的全部元素。例如，

α 是 $x^4+x+1=0$ 的根，即 $\alpha^4=\alpha+1$，从而

$$\alpha^5=\alpha^2+\alpha$$

再注意 α 是 $x^2+x+\xi=0$ 的根，即 $\alpha^2=\alpha+\xi$，故

$$\alpha^5=(\alpha+\xi)+\alpha=\xi$$

由此

$$\alpha^{10}=(\alpha^5)^2=\xi^2=\partial$$

余此类推。我们可以找出 α 的各次幂在 $GF(16)$ 中所对应的元素（参看表 5-1）。

我们也可以选择另外一个本原域元素，例如 $x^2+\xi x+\xi=0$ 的根 β 来表示 $GF(16)$。由于 $\beta=\alpha^7$，故有

$$\beta^2=\alpha^{14},\ \beta^3=\alpha^6,\ \beta^4=\alpha^{13},\ \cdots$$

第二种方法是将 $GF(16)$ 表示为 $GF(2)$ 上次数低于 4 的 α 的全体多项式的集合。

由于 α 是 $GF(2)$ 上的 4 次既约多项式 x^4+x+1 的根，根据定理 5.5.4，系数在 $GF(2)$ 上的所有次数低于 4 的 α 的多项式便构成 $GF(16)$。每一个这种 α 的多项式皆对应 α 的一个幂，例如

$$0110=0\cdot\alpha^3+1\cdot\alpha^2+1\cdot\alpha+0\cdot1=\alpha^2+\alpha$$
$$=\xi=\alpha^5$$

余此类推（参看表 5-1）。这些元素可以通过逐次乘以 α 的反馈移位寄存器获得。

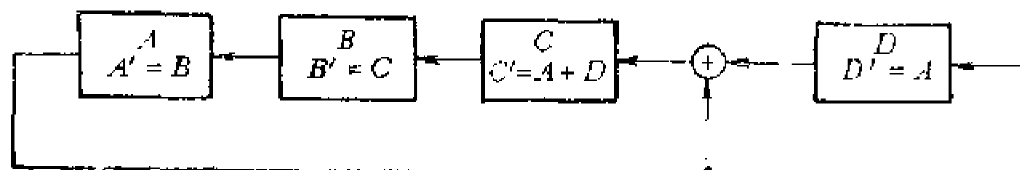

图 5-3

在图 5-3 中，假定寄存器原来的状态是

$$A\alpha^3+B\alpha^2+C\alpha+D \quad (A,\ B,\ C,\ D=0\text{ 或 }1)$$

移位脉冲一来，它就变成下一个状态

$$A'\alpha^3+B'\alpha^2+C'\alpha+D'$$
$$=\alpha\,(A\alpha^3+B\alpha^2+C\alpha+D)$$
$$=A\alpha^4+B\alpha^3+C\alpha^2+D\alpha$$
$$=A(\alpha+1)+B\alpha^3+C\alpha^2+D\alpha$$
$$=B\alpha^3+C\alpha^2+(A+D)\alpha+A$$

即

$$A'=B,\ B'=C,\ C'=A+D,\ D'=A$$

例如，$\alpha^5=0110$ 的下一个状态是

$$1100=\alpha^3+\alpha^2=\alpha^2(\alpha+1)=\alpha^2\cdot\alpha^4=\alpha^6$$

因此从$\alpha^0=0001$ 出发，经过上述反馈移位寄存器就可以获得 α 逐次幂的二进制多项式表示。

这种表示方法是目前数字电路中最常用的。

第三种方法是所谓对数表示方法。

例如，从

$$\alpha^5=\xi,\ \alpha^{10}=\partial$$

我们可以写成

$$\log_\alpha\xi=5=0101,\ \log_\alpha\partial=10=1010$$

（十进制）　　　（十进制）

因此，当我们把 α 的各次幂的幂指数表示成 4 位二进制数时，就得到$GF(16)$ 的全部元素的对数表示。

对数表示方法有两个重要的优点

第一，乘法逆元素的二进制对数等于原来元素二进制对数的逐位取补。

设 $x=\alpha^m$，则$x^{-1}=\alpha^{-m}=\alpha^{15-m}$。于是，

$$\log_\alpha x=m,\ \log_\alpha x^{-1}=15-m$$

例如，设$m=5$，则

$$\log_\alpha x=5=0101$$

而

$$\log_\alpha x^{-1}=15-5=10=1010$$

它刚好是0101的逐位取补（即 $0\to1$，$1\to0$）。

第二，任意域元素的全体共轭元素均可由其中一个元素循环左移而得到。

例如，$w=\alpha^{11}$ 为 15 阶域元素，由于 2 的模 15 阶为 4，故 w 为 4 次域元素。w 的共轭元素系是

$$w=\alpha^{11},\quad w^2=\alpha^{22}=\alpha^7,\quad w^4=\alpha^{14},\quad w^8=\alpha^{13}$$

我们有

$$\log_\alpha w=11=1011,\quad \log_\alpha w^2=7=0111$$
$$\log_\alpha w^4=14=1110,\quad \log_\alpha w^8=13=1101$$

显然由 1011 逐次循环左移，即得

$$0111,\quad 1110,\quad 1101$$

在结束本节之前，我们作一个注记。理论上，我们可以将 $GF(16)$ 表示成 $GF(2)$ 上任意一个 4 次既约多项式的根的低于 4 次的多项式。但如果该多项式不是本原多项式表示时，就带来诸多不便。例如，$\gamma=\alpha^3$是方程$x^4+x^3+x^2+x+1=0$ 的根，是 5 阶 4 次域元素。由于$\gamma^5=1$，故我们无法将$GF(16)$ 中的全体元素表示成 γ 的幂的形式。但是我们可以通过 γ 的幂及其陪集来表示$GF(16)$ 中所有的元素（见表 5-2）。

在将$GF(16)$ 中的元素表示成 γ 的低于 4 次的多项式时，首先有

$$1=0001,\quad \gamma=0010,\quad \gamma^2=0100,$$
$$\gamma^3=1000,\quad \gamma^4=1111$$

注意到

$$\gamma=\alpha^3\quad \gamma^2=\alpha^6=\alpha^3+\alpha^2\quad \gamma^3=\alpha^9=\alpha^3+\alpha$$

故

$$\alpha\gamma^0=\gamma^3+\gamma=1010$$
$$\varphi\gamma^0=\alpha^2=\gamma^2+\gamma=0110$$

余此类推。

考虑如图 5-4 所示的逐次乘以 γ 的反馈移位寄存器。从任意一个初始状态出发，寄存器将依次通过该初态所在的陪集中的其它 4 个状态，然后返回初态。例如，当初态为 $1010=\alpha\gamma^0$ 时，由

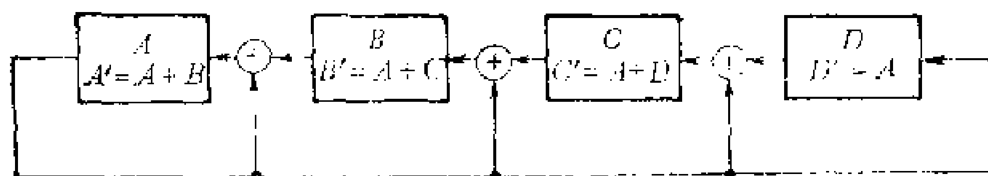

图 5-4

于$A'=A+B$，$B'=A+C$，$C'=A+D$，$D'=A$，故下一状态为

$$1011=\gamma^3+\gamma+1=\alpha+1=\alpha^4=\alpha\gamma$$

接下来是

$$1001=\gamma^3+1=\alpha^3+\alpha+1=\alpha^7=\alpha\gamma^2$$

$$1101=\gamma^3+\gamma^2+1=\alpha^2+\alpha+1=\alpha^{10}=\alpha\gamma^3$$

$$0101=\gamma^2+1=\alpha^3+\alpha^2+1=\alpha^{13}=\alpha\gamma^4$$

最后返回初态　$1010=\alpha\gamma^0$

§5.9　最小多项式的求法

在前一节的例子中，我们已经求出了$GF(16)$中全体元素（在$GF(2)$上）的最小多项式。设α为本原多项式x^4+x+1的根，如果我们用$m^{(i)}(x)$表示α^i的最小多项式，由$\alpha^4+\alpha+1=0$定义的$GF(2^4)$见表5-3。

由定理5.8.1易得，α的最小多项式为$m(x)$当且仅当α^{-1}的最小多项式为$\widetilde{m}(x)$。因此，在表5-3中有

$$m^{(14)}(x)=m^{(15-1)}(x)=m^{(-1)}(x)=\widetilde{m}^{(1)}(x)$$
$$=x^4+x^3+1$$

上述结论在求最小多项式时十分有用。

由上表我们还看出，本原多项式x^4+x+1的根的各次幂都分属于互不相交的集合，我们称为分圆陪集。当i，j属于同一个分圆陪集时，α^i和α^j有相同的最小多项式。

定义5.9.1　设s为整数，且$0\leqslant s<p^m-1$，而r是满足$p^{r+1}s\equiv s\pmod{p^m-1}$的最小正整数，则称集合$\{s，ps，p^2s，$

表 5-2

α 的 幂		α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
$GF(16)$的全部元素	0	1	α	φ	ν	π	ξ	δ	β	ρ	μ	∂	λ	θ	ϑ	ζ
$GF(2)$ 上 α 的多项式	0000	0001	0010	0100	1000	0011	0110	1100	1011	0101	1010	0111	1110	1111	1101	1001
二进制对数		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110
β 的 幂		β^0	β^{13}	β^{11}	β^{9}	β^7	β^5	β^3	β^1	β^{14}	β^{12}	β^{10}	β^8	β^6	β^4	β^2
$GF(2)$ 上 β 的多项式	0000	0001	0110	1101	0101	0111	1011	1000	0010	1100	0011	1010	1110	1111	1001	0100
γ 的 幂		γ^0			γ^1			γ^2			γ^3			γ^4		
γ 的幂的陪集表示	0	γ^0	$\alpha\gamma^0$	$\varphi\gamma^0$	γ	$\alpha\gamma$	$\varphi\gamma$	γ^2	$\alpha\gamma^2$	$\varphi\gamma^2$	γ^3	$\alpha\gamma^3$	$\varphi\gamma^3$	γ^4	$\alpha\gamma^4$	$\varphi\gamma^4$
$GF(2)$ 上 γ 的多项式	0000	0001	1010	0110	0010	1011	1100	0100	1001	0111	1000	1101	1110	1111	0101	0011

表 5-3

元素	最小多项式
0	x
1	$m^{(0)}(x)=x+1$
α, α^2, α^4, α^8	$m^{(1)}(x)=m^{(2)}(x)=m^{(4)}(x)=m^{(8)}(x)=x^4+x+1$
α^3, α^6, α^{12}, α^9	$m^{(3)}(x)=m^{(6)}(x)=m^{(12)}(x)=m^{(9)}(x)=x^4+x^3+x^2+x+1$
α^5, α^{10}	$m^{(5)}(x)=m^{(10)}(x)=x^2+x+1$
α^7, α^{14}, α^{13}, α^{11}	$m^{(7)}(x)=m^{(14)}(x)=m^{(13)}(x)=m^{(11)}(x)=m^{(-1)}(x)=x^4+x^3+1$

…, $p^r s\}$ 为模 p^m-1 的包含 s 的分圆陪集，其中各 $p^i s$ 均对 p^m-1 取模。

例如，在$GF(2)$上，模 15 的分圆陪集为

$$C_0=\{0\}$$
$$C_1=\{1, 2, 4, 8\}$$
$$C_3=\{3, 6, 12, 9\}$$
$$C_5=\{5, 10\}$$
$$C_7=\{7, 14, 13, 11\}$$

其中 C_s 表示该陪集中最小的元素为 s，并称 s 为该陪集的代表元。

若 α^i 为 k 次域元素，则$|C_i|=k$。例如，α^5 是$GF(2^4)$中的 $\frac{15}{(5,15)}=3$ 阶元素，而 2 的模 3 阶为 2，故α^5是 2 次域元素，因此$|C_5|=2$。

再举两个$GF(2)$上分圆陪集的例子

mod 7	mod31
$C_0=\{0\}$	$C_0=\{0\}$
$C_1=\{1, 2, 4\}$	$C_1=\{1, 2, 4, 8, 16\}$
$C_3=\{3, 6, 5\}$	$C_3=\{3, 6, 12, 24, 17\}$

$$C_5=\{5, 10, 20, 9, 18\}$$
$$C_7=\{7, 14, 28, 25, 19\}$$
$$C_{11}=\{11, 22, 13, 26, 21\}$$
$$C_{15}=\{15, 30, 29, 27, 23\}$$

设 α 是$GF(2^3)$ 上本原多项式 x^3+x+1 的根，则 α，α^2，α^4 的最小多项式显然是x^3+x+1，而α^3，α^6，α^5 的最小多项式则为 $m^{(6)}(x)=m^{(7-1)}(x)=m^{(-1)}(x)=\widetilde{m}^{(1)}(x)=x^3+x^2+1$。因而由$\alpha^3+\alpha+1=0$ 定义的$GF(2^3)$ 见表 5-4。

表　5-4

元　素	最　小　多　项　式
0	x
1	$m^{(0)}(x)=x+1$
α，α^2，α^4	$m^{(1)}(x)=m^{(2)}(x)=m^{(4)}(x)=x^3+x+1$
α^3，α^6，α^5	$m^{(3)}(x)=m^{(6)}(x)=m^{(5)}(x)=m^{(-1)}(x)=x^3+x^2+1$

注意到

$$\alpha^3=\alpha+1,\ \alpha^4=\alpha^2+\alpha,\ \cdots$$

我们可以直接计算 α^3 的最小多项式为

$$\begin{aligned}&(x+\alpha^3)(x+\alpha^6)(x+\alpha^5)\\&=(x^2+(\alpha^2+\alpha)x+\alpha^2)(x+\alpha^6)\\&=x^3+x^2+1\end{aligned}$$

顺便指出，我们可以用下面的方法证明x^3+x+1是$GF(2^3)$上的本原多项式。因为本原多项式的计数公式是

$$\frac{\varphi(2^m-1)}{m}，（在GF(2^m) 上）$$

故当$m=3$时，$GF(2^3)$ 中共有$\frac{\varphi(7)}{3}=2$个本原多项式。由例5.7.1可知，$GF(2)$ 上共有 2 个 3 次既约多项式，因此 2 个 3 次既约多项式

$$x^3+x+1,\ x^3+x^2+1$$

都是本原多项式。根据同样的原因，$GF(2)$ 上的 6 个 5 次既约多项式都是$GF(2^5)$ 中的本原多项式。

一般地，我们有

定理5.9.1 当2^m-1为素数时，$GF(2)$ 上任意m次既约多项式皆为m次本原多项式。

证明 首先证明当 2^m-1 为素数时，m必为素数。假定不然，令$m=pq(1<p,\ q<m)$，则有

$$2^m-1=2^{pq}-1=(2^p-1)(2^{p(q-1)}+\cdots+2^p+1)$$

产生矛盾。

因此

$$I_2(m)=\frac{2^m-2}{m}=\frac{\varphi(2^m-1)}{m}$$

〈证毕〉

在数论中，称形如 2^m-1 的素数为默森尼（Mersenne）素数 可惜，这种素数是很少的。目前仅知道 29 个默森尼素数，其对应的m值为

2，3，5，7，13，17，19，31，61，89，107，

127，521，607，1279，2203，2281，3217，4253，

4423，9689，9941，11213，19937，21701，

23209，44497，86243，132049

注意当m为素数时，2^m-1可能是合数。例如，$2^{11}-1=2047=23\times89$

一般而言，求本原多项式是很困难的。

下面我们介绍从已知的最小多项式求其它元素的最小多项式的方法。

定理5.9.2 〔路卡斯（Lucas)〕 设p为素数，且

$$N=\sum_{i=0}^{l}N_ip^i,\quad 0\leqslant N_i<p$$

$$k=\sum_{i=0}^{I} k_i p^i,\quad 0\leqslant k_i<p$$

则

$$\binom{N}{k}\equiv\prod_{i=0}^{I}\binom{N_i}{k_i}\pmod p$$

证明　由定理5.4.4得

$$(1+x)^p=\sum_{k=0}^{p}\binom{p}{k}x^k\equiv 1+x^p\pmod p$$

于是，

$$(1+x)^{np+A}\equiv(1+x^p)^n(1+x)^A\pmod p$$

亦即

$$\sum_{m=0}^{np+A}\binom{np+A}{m}x^m\equiv\left(\sum_{i=0}^{n}\binom{n}{i}x^{pi}\right)\left(\sum_{j=0}^{A}\binom{A}{j}x^j\right)\pmod p$$

等式两边形如x^{kp+B}的项的系数应当相等。注意到，当$0\leqslant A<B<p$时，等式右边不可能出现x^{kp+B}这种类型的项，因而有

$$\binom{np+A}{kp+B}\equiv\begin{cases}0 & 若\ 0\leqslant A<B<p\\ \binom{n}{k}\binom{A}{B} & 若\ 0\leqslant B<A<p\end{cases}$$

我们定义，对于$A<B$，恒有

$$\binom{A}{B}=0$$

于是

$$\binom{np+A}{kp+B}\equiv\binom{n}{k}\binom{A}{B}\pmod p$$

对任意$0\leqslant A$，$B<p$均成立。

由此可见，当$I=2$时，定理成立。用归纳法容易证明定理的正确性。　　　　（证毕）

推论5.9.2.1 在定理5.9.2的条件下，只要有一个$k_i > N_i$，$i=0$，1，2，…，I，则有

$$\binom{N}{k} \equiv 0 \pmod{p}$$

证明 由定理5.9.2即得。

注意，当p不是素数时，定理并不成立。例如，当$p=10$时，$\binom{14}{12} \equiv 1 \pmod{10}$，而$\binom{1}{1}\binom{4}{2} \equiv 6 \pmod{10}$。

设已知α的最小多项式为$m(x)$，则$\alpha-k$的最小多项式$\hat{m}(x)$必有如下性质：

$\hat{m}(u)=0$，当且仅当$m(u+k)=0$

因此，$\hat{m}(x)=m(x+k)$。当k是正整数时，我们就可以利用二项式定理直接求出$\hat{m}(x)$

$$\hat{m}(x)=m(x+k)=\sum_n m_n(x+k)^n=\sum_n m_n \sum_i \binom{n}{i} x^{n-i}k^i$$

并在p特征域中，通过路卡斯定理简化上面的计算过程。

例5.9.1 设α为$GF(2^5)$中的元素，且α在$GF(2)$上的最小多项式为$m(x)=x^5+x^2+1$。求$\alpha^{18}=\alpha+1$的最小多项式。

在$GF(2)$中，计算过程特别简单。根据推论5.9.2.1，可以列表（5-5）计算。

表 5-5

	101	100	11	10	1	0
$(x+1)^{101}$	1	1	0	0	1	1
$(x+1)^{10}$				1	0	1
1						1
模 2 和	1	1	0	1	1	1

因此，$\hat{m}(x)=x^5+x^4+x^2+x+1$。参见后面的表5-7，当$m^{(1)}(x)=x^5+x^2+1$时，恰有

$$m^{(15)}(x)=x^5+x^4+x^2+x+1$$

已知 α 的最小多项式为 $m^{(1)}(x)$，常常需要计算 α^k 的最小多项式 $m^{(k)}(x)$。在特征为 2 的域上，当 $k=3$ 时，我们有下述定理。

定理5.9.3 设 ∂ 是 $GF(4)$ 中的本原域元素，则 $m^{(1)}(x)m^{(1)}(\partial x)m^{(1)}(\partial^2 x)$ 是 $m^{(3)}(x^3)$ 的方幂。

证明 若 $m^{(1)}(\alpha)=0$，则 $m^{(3)}(\alpha^3)=0$，故 $m^{(1)}(x)|m^{(3)}(x^3)$。由于 $\partial^3=1$，故类似地有 $m^{(1)}(\partial x)|m^{(3)}(x^3)$ 和 $m^{(1)}(\partial^2 x)|m^{(3)}(x^3)$。另一方面，$m^{(3)}(x^3)$ 的根必为 $m^{(1)}(x)$，$m^{(1)}(\partial x)$ 和 $m^{(1)}(\partial^2 x)$ 中的一个根。（证毕）

设 $m^{(1)}(x)=A+B+C$，其中 $A=A(x^3)$，$B=xB(x^3)$，$C=x^2C(x^3)$，则 $m^{(1)}(\partial x)=A(x^3)+\partial xB(x^3)+\partial^2x^2C(x^3)=A+B\partial+C\partial^2$。同理可得，$m^{(1)}(\partial^2 x)=A+B\partial^2+C\partial$。因此

$$\begin{aligned}&m^{(1)}(x)m^{(1)}(\partial x)m^{(1)}(\partial^2 x)\\&=(A+B+C)(A+B\partial+C\partial^2)(A+B\partial^2+C\partial)\\&=ABC+A^3+B^3+C^3\end{aligned}$$

在上述化简过程中，利用了下述事实：

$$\partial^2=\partial+1$$

有了上面的公式，从 $m^{(1)}(x)$ 计算 $m^{(3)}(x)$ 就不会有什么困难了。

例5.9.2 计算 $GF(2^5)$ 中全体元素的最小多项式。已知 $m^{(1)}(x)=x^5+x^2+1$，我们首先求出 $m^{(3)}(x)$，然后重复上述计算过程求出 $m^{(9)}(x)$。表 5-6 列出了 $m^{(1)}(x)=x^5+x^2+1$ 和 $m^{(3)}(x)=x^5+x^4+x^3+x^2+1$ 的立方变换过程，其中仅列出了幂指数。

我们仅对由 $m^{(3)}(x)$ 计算 $m^{(9)}(x)$ 的过程予以说明。这时有

$$A=1+x^3,\quad B=x^4,\quad C=x^2+x^5$$

首先在 A、B 和 C 列写出 $m^{(3)}(x)$ 中分别与 0、1 和 2 模 3 同余的幂指数。在本例中，我们在 A 列写 0 和 3，在 B 列写 4，在 C 列写 2 和 5。

表 5-6

	A	B	C
$m^{(1)}(x)$	0		2， 5
$\frac{\text{立方交叉相乘项}}{3}C^3$	3	4	
$\frac{ABC}{3}$			
$m^{(3)}(x)$	0， 3	4	2， 5
$\frac{\text{立方交叉相乘项}}{3}$ A^3		1	2
C^3	3	4	
$\frac{ABC}{3}$	3， 3	4	2
$m^{(9)}(x)$	0	1， 4	2， 5

然后分别计算A^3、B^3和 C^3。一般地，我们有 $A=\sum_i A_i x^i$，故

$$A^3=\left(\sum_i A_i x^i\right)^3=\left(\sum_i A_i x^i\right)\left(\sum_j A_j x^j\right)^2$$

$$=\left(\sum_i A_i x^i\right)\left(\sum_j A_j x^{2j}\right)=\sum_i A_i x^{3i}+\sum_{i\neq j}\sum A_i A_j x^{i+2j}$$

当幂指数除以 3 时，上面第一个和式 $\sum_i A_i x^{3i}$ 即为A；第二个和式称为立方交叉相乘项，它的一般形式为

$$x^{i+2j}$$

其中$A_i=A_j=1$，$i\neq j$。在本例中，交叉相乘项为 $0+2\times3=6$ 和 $3+2\times0=3$，除以 3 后得 2 和 1，如表 5-6 所示。类似地，可以计算C^3的立方交叉相乘项。它们是 $2+2\times5=12$和 $5+2\times2=9$，除以 3 后得 4 和 3，也将它们列入表 5-6 中。

接着计算ABC中的诸项。本例共有 4 项，即 $0+4+2=6$，$0+4+5=9$，$3+4+2=9$，$3+4+5=12$。除以 3 后得 2、3、3 和 4，如表5-6所示。

最后计算表5-6中各列的模2和，我们得到0、1、2、4、5。因此，$m^{(3)}(x)m^{(3)}(\alpha x)m^{(3)}(\alpha^2 x)=1+x^3+(x^3)^2+(x^3)^4+(x^3)^5$，亦即$1+x+x^2+x^4+x^5$是$m^{(3)}(x)$的某次幂。由于$x^5+x^4+x^2+x+1$是既约多项式，于是

$$m^{(3)}(x)=x^5+x^4+x^2+x+1$$

通过互反多项式，易得其它3个最小多项式。

$$m^{(-1)}(x)=m^{(30)}(x)=x^5(x^{-5}+x^{-2}+1)$$
$$=x^5+x^3+1$$
$$m^{(-3)}(x)=m^{(28)}(x)=x^5(x^{-5}+x^{-4}+x^{-3}+x^{-2}+1)$$
$$=x^5+x^3+x^2+x+1$$
$$m^{(-9)}(x)=m^{(22)}(x)=x^5(x^{-5}+x^{-4}+x^{-2}+x^{-1}+1)$$
$$=x^5+x^4+x^3+x+1$$

由$\alpha^5+\alpha^2+1=0$定义的$GF(2^5)$如表5-7所示。

表 5-7

α的幂指数所属的分圆陪集	最　小　多　项　式
C_0	$m^{(0)}(x)=x+1$
C_1	$m^{(1)}(x)=m^{(2)}(x)=m^{(4)}(x)=m^{(8)}(x)=m^{(16)}(x)=x^5+x^2+1$
C_3	$m^{(3)}(x)=m^{(6)}(x)=m^{(12)}(x)=m^{(24)}(x)=m^{(17)}(x)=x^5+x^4+x^3+x^2+1$
C_5	$m^{(5)}(x)=m^{(10)}(x)=m^{(20)}(x)=m^{(9)}(x)=m^{(18)}(x)=x^5+x^4+x^2+x+1$
C_7	$m^{(7)}(x)=m^{(14)}(x)=m^{(28)}(x)=m^{(25)}(x)=m^{(19)}(x)=m^{(-3)}(x)=x^5+x^3+x^2+x+1$
C_{11}	$m^{(11)}(x)=m^{(22)}(x)=m^{(13)}(x)=m^{(26)}(x)=m^{(21)}(x)=m^{(-9)}(x)=x^5+x^4+x^3+x+1$
C_{15}	$m^{(15)}(x)=m^{(30)}(x)=m^{(29)}(x)=m^{(27)}(x)=m^{(23)}(x)=m^{(-1)}(x)=x^5+x^3+1$

在本节的最后，我们介绍一种求最小多项式的一般方法，这种方法很容易在计算机上编程实现。

例如，γ是$GF(2)$上的既约多项式$x^4+x^3+x^2+x+1$在

$GF(16)$ 中的根，我们欲求 $\alpha=\gamma+\gamma^{3}$ 的最小多项式。

注意到，$\gamma^{4}=\gamma^{3}+\gamma^{2}+\gamma+1$，我们有

$$\left.\begin{array}{llll} 1=1 & & & \\ \alpha= & \gamma & & +\gamma^{3} \\ \alpha^{2}= & \gamma+\gamma^{2} & & \\ \alpha^{3}= & \gamma & & \\ \alpha^{4}=1+ & \gamma & & +\gamma^{3} \end{array}\right\}$$

设 α 的最小多项式为

$$m(x)=m_0+m_1x+m_2x^2+m_3x^3+m_4x^4$$

因为

$$m(\alpha)=0$$

故有

$$(m_0\ m_1\ m_2\ m_3\ m_4)\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}=(0\ \ 0\ \ 0\ \ 0)$$

解方程

$$\left.\begin{array}{l} m_0+m_4=0 \\ m_1+m_2+m_3+m_4=0 \\ m_3=0 \\ m_1+m_4=0 \end{array}\right\}$$

得

$$m_3=m_2=0,\quad m_0=m_1=m_4=1$$

因此，α 的最小多项式是

$$m(x)=x^4+x+1$$

§5.10 多项式的周期

多项式周期的概念是编码理论中一个十分有用的概念。

定义 5.10.1 设 $f(x)\in GF(q)[x]$，且 $f(0)\neq 0$，我

们称使 $f(x)|x^l-1$ 成立的最小正整数 l 为 $f(x)$ 的周期，并记为 $p(f)$。

注意这里 $f(0)\neq 0$ 的假定是必要的。否则，当 $f(0)=0$ 时，$f(x)$ 必不能整除任何 x^l-1，从而 $f(x)$ 的周期不存在。

我们知道，$GF(q)[x]$ 中的多项式按模 $f(x)$ 构成剩余类环 $GF(q)[x]\bmod f(x)$。与定理 3.2.8 完全类似，剩余类环 $GF(q)[x]\bmod f(x)$ 中那些与 $f(x)$ 互素的剩余类集合构成阿贝尔乘法群，记此群为 $(GF(q)[x]\bmod f(x))^*$。由于 $GF(q)$ 为有限域，故此乘法群亦为有限群。因此在该群中元素 $x \bmod f(x)$ 之阶必为有限。注意因 $f(0)\neq 0$，故 $(x, f(x))=1$。

定理5.10.1 $f(x)$ 的周期 l 是乘法群 $(GF(q)[x]\bmod f(x))^*$ 中的元素 $x\bmod f(x)$ 之阶。

证明 若 $p(f)=l$，则 l 是使 $f(x)|(x^l-1)$ 的最小正整数。因此 $x\bmod f(x)$ 在乘法群 $(GF(q)[x]\bmod f(x))^*$ 中的阶为 l。（证毕）

由此定理，对于 $GF(q)[x]$ 中的任意多项式 $f(x)$，只要 $f(0)\neq 0$，它的周期总是存在的。

推论5.10.1.1 设 $f(x)\in GF(q)[x]$，$f(0)\neq 0$，则 $f(x)|(x^l-1)$ 当且仅当 $p(f)|l$。

证明 若 $f(x)|(x^l-1)$，则

$$x^l\equiv 1 \pmod{f(x)}$$

由定理 3.3.5 及定理 5.10.1，立即推得 $p(f)|l$。反之，若 $p(f)|l$，则仍由定理 3.3.5 和定理 5.10.1 得，$x^l\equiv 1 \pmod{f(x)}$，即 $f(x)|(x^l-1)$。（证毕）

对于既约多项式，则有

定理5.10.2 设 $f(x)$ 为 $GF(q)[x]$ 中的 m 次既约多项式，则 $f(x)$ 的周期等于 $f(x)$ 在 $GF(q^m)$ 中的根的阶。

证明 由定理 3.6.3，$GF(q)[x]\bmod f(x)$ 构成域。因

此，$f(x)$ 的全部根都在$GF(q^m)$之中。根据定理5.6.2，$\bar{x}=x \bmod f(x)$ 即为 $f(x)$ 的一个根。由定理5.10.1，$f(x)$的周期就是x的阶。（证毕）

类似于引理5.6.1，我们有

引理5.10.1 在任意域上，恒有

$(x^m-1)|(x^n-1)$当且仅当$m|n$。

证明 留作习题。

引理5.10.2 设$(a,\ p)=1$，则p特征域上的多项式$f(x)=x^a-1$没有重因式。

证明 因为$(a,\ p)=1$，故

$$f'(x)=ax^{a-1}\neq 0$$

$f'(x)$ 只有x一个既约因式，且$x\nmid(x^a-1)$，故$(f(x),\ f'(x))=1$。因此由定理3.1.13，$f(x)=x^a-1$没有重因式。

（证毕）

引理5.10.3 设$f(x)$为$GF(q)[x]$中的既约因式，且$f(0)\neq 0$，则

$$(p(f),\ p)=1$$

证明 由定理5.6.4及条件$f(0)\neq 0$，有

$$f(x)|(x^{q^n-1}-1)$$

因此，根据推论5.10.1.1，

$$p(f)|(q^n-1)$$

显然$p\nmid(q^n-1)$，故$p\nmid p(f)$，因此

$$(p,\ p(f))=1$$

（证毕）

下述定理对于多项式周期的计算是十分有用的。

定理5.10.3 设$GF(q)$为p特征域，$f(x)=\prod_{i=1}^{t}f_i^{m_i}(x)$是$f(x)$在$GF(q)[x]$上的既约因式分解，并且

$$p(f_i)=n_i,\quad i=1,\ 2,\ \cdots,\ t$$

则

$$p(f)=n\cdot p^d$$

其中

$$n=[n_1,\ n_2,\ \cdots,\ n_l]$$
$$d=\lceil \log_p(\max\{m_1,\ m_2,\ \cdots,\ m_l\})\rceil$$

此处用符号$\lceil x\rceil$表示$\geqslant x$的最小整数。例如，$\lceil 3.5\rceil=4$。

证明 我们分三步证明。

(1) 设$f(x)$是既约多项式，且$p(f)=n$，则

$$p(f^m)=p(f)\cdot p^d$$

其中$d=\lceil\log_p m\rceil$。下面，证明这一论断的正确性。

由假设

$$p^d\geqslant m\ 且\ p^{d-1}<m \tag{5-26}$$

由于

$$f^m(x)|(x^{p(f)}-1)^m$$

故

$$f^m(x)|(x^{p(f)}-1)^{p^d}=(x^{p^d\cdot p(f)}-1)$$

因此

$$p(f^m)|p^d\cdot p(f) \tag{5-27}$$

反过来设$p(f^m)=p^b\cdot a$，其中$(a,\ p)=1$，则有

$$f^m(x)|(x^{p^b\cdot a}-1)=(x^a-1)^{p^b}$$

根据引理5.10.2，x^a-1没有重因式，且$f(x)$是既约多项式，故由定理3.1.9，得

$$f(x)|(x^a-1)$$

并且

$$m\leqslant p^b \tag{5-28}$$

因此

$$p(f)|a$$

由式(5-26)和式(5-28)，我们有

$$p^b\geqslant p^d$$

所以

$$p(f^m)=p^b\cdot a\geqslant p^a\cdot p(f) \qquad (5\text{-}29)$$

综合式（5-27）及式（5-29），即得所欲证。

（2）设 $f(x)=f_1(x)f_2(x)$，其中 $(f_1(x),\ f_2(x))=1$，我们证明

$$p(f)=[p(f_1),\ p(f_2)]$$

设 $a=[p(f_1),\ p(f_2)]$，由引理5.10.1，得

$$f_1(x)|(x^a-1),\ f_2(x)|(x^a-1)$$

因为

$$(f_1(x),\ f_2(x))=1$$

故

$$f_1(x)f_2(x)|(x^a-1)$$

因此

$$p(f)|a \qquad (5\text{-}30)$$

反过来，由于

$$f_1(x)|(x^{p(f)}-1),\ f_2(x)|(x^{p(f)}-1)$$

故

$$p(f_1)|p(f),\ p(f_2)|p(f)$$

因此

$$a|p(f) \qquad (5\text{-}31)$$

综合式（5-30）与式（5-31），命题得证。

利用归纳法，容易将上述结果推广到 I 个两两互素的多项式相乘的情形。

（3）根据（1）和（2）中的结果，有

$$\begin{aligned}p(f)&=[p(f_1^{m_1}),\ p(f_2^{m_2}),\ \cdots,\ p(f_I^{m_I})]\\&=[p(f_1)\cdot p^{d_1},\ p(f_2)\cdot p^{d_2},\ \cdots,\ p(f_I)p^{d_I}]\end{aligned}$$

其中 $d_i=\lceil\log_p m_i\rceil$，$i=1,\ 2,\ \cdots,\ I$

由引理5.10.3，$(p(f_i),\ p)=1$，$i=1,\ 2,\ \cdots,\ I$，因此●

● 请读者证明，当 $(a,\ p)=(b,\ p)=1$，且 $r\leqslant s$ 时，恒有 $(ap^r,\ bp^s)=(a,\ b)\cdot p^r$，$[ap^r, bp^s]=[a,\ b]\cdot p^r$。

$$[p(f_1)\cdot p^{d_1},\ p(f_2)\cdot p^{d_2},\ \cdots,\ p(f_l)p^{d_l}]$$
$$=[p(f_1),\ p(f_2),\ \cdots,\ p(f_l)]\cdot p^d$$

其中 $d=\max\{d_1, d_2, \cdots, d_l\}$。 （证毕）

推论5.10.3.1 在定理5.10.3中，当$m_i=1$（$i=1, 2, \cdots, l$）时，有

$$p(f)=[n_1, n_2, \cdots, n_l]$$

证明 由 $d=\lceil\log_p(\max\{m_1, m_2, \cdots, m_l\})\rceil=\lceil\log_p 1\rceil=0$，即得此推论。 （证毕）

设$g(x)$是循环码C的生成多项式，且$p(g)=n$，则由$x^n-1=g(x)h(x)$可知，$C=\langle g(x)\rangle$的最小分组长$n=p(g)$。

例5.10.1 求以

$$g(x)=(x^4+x^3+x^2+x+1)(x^4+x+1)$$

为生成多项式的二元循环码的最小分组长。

解 这相当于求$p(g)$。

我们知道，$g_1(x)=x^4+x^3+x^2+x+1$是$GF(2)$上的4次既约多项式，它在$GF(2^4)$中的根是5阶元素，因此$p(g_1)=5$。而$g_2(x)=x^4+x+1$是$GF(2)$上的4次本原多项式，故$p(g_2)=2^4-1=15$。由推论5.10.3.1，得

$$p(g)=[5, 15]=15$$

例5.10.2 求$GF(2)$上的多项式

$$f(x)=(x+1)^3(x^4+x^3+x^2+x+1)(x^4+x+1)$$

的周期。

解 显然$GF(2)$上的既约多项式$x+1$的周期为1。因此由定理5.10.3得

$$p(f)=[1, 5, 15]\times 2^2=15\times 4=60$$

关于有限域的基本理论，就介绍到这里。作为有限域理论的直接应用，下一节我们讨论双纠错BCH码。

§5.11 二元双纠错BCH码

从第二章的讨论我们知道，50年代初期建立的纠正一个独立错误的汉明码是一种典型的"好"码。很自然地，人们希望设计出类似于汉明码的、能纠正多个独立错误的码类。这个工作远比想象的要困难得多，经过了约10年的时间，纠正多个错误的码才由波斯（Bose），卓乎利（Chauduri）和荷昆汉姆(Hocquenhem)独立地确定，这就是我们现在所说的BCH码。

为了说明由单纠错码到多纠错码的转变过程，我们考虑如何建立码长 $n=2^4-1=15$的二元双纠错BCH码的问题。

回忆二元（15.11）汉明码的一致校验矩阵，形如

$$H=\begin{pmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix}$$

其中没有全零列，且各列互不相同。

设α是$GF(2)$上4次本原多项式x^4+x+1的根，则根据表5-2，可使H中的各列与α的方幂相对应。例如，

$$1=\begin{pmatrix}0\\0\\0\\1\end{pmatrix},\quad \alpha=\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\quad \alpha^2=\begin{pmatrix}0\\1\\0\\0\end{pmatrix},\quad \cdots$$

等等。这里只不过将表5-2中表示α的方幂的行向量转置成列向量而已。

为方便起见，我们对H矩阵进行列置换，使H中的各列按α的升幂排列，因而得到下面的等价码的一致校验矩阵，

$$H_1=(1 \quad \alpha \quad \alpha^2 \quad \cdots \quad \alpha^{14})$$

$$=\begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

我们从 H_1 矩阵出发，试图建立一个双纠错码的一致校验矩阵H'。

显然双纠错码比单纠错码需要更多的校验位。因此，我们应该增加H'中的行数。不妨将H_1的行数加倍，使H'具有形状

$$H'=\begin{pmatrix} 1 & \alpha & \cdots & \alpha^{14} \\ f(1) & f(\alpha) & \cdots & f(\alpha^{14}) \end{pmatrix}$$

其中 f 是$GF(2^4)$ 到$GF(2^4)$ 上的某个待定的一一映射。

为了实现由单纠错码到双纠错码这一质的转变，关键在于选择 f。由 §2.6 我们知道，接收向量的伴随式等于一致校验矩阵中与信道错误相对应的各列之和。因此，如果接收向量 $\boldsymbol{r}=(r_0, r_1, \cdots, r_i, \cdots, r_j, \cdots, r_{n-1})$ 中的 r_i 和 r_j 出错（即第 i 和第 j 位出错），则$\boldsymbol{r}$的伴随式$\mathbf{s}'$为

$$\mathbf{s}'=\begin{pmatrix} \alpha^i+\alpha^j \\ f(\alpha^i)+f(\alpha^j) \end{pmatrix}\triangleq\begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

于是，我们的问题转化为选择 f，使得当给定R_1和R_2之后，可以解出关于 i 和 j 的方程

$$\left.\begin{aligned} \alpha^i+\alpha^j=R_1 \\ f(\alpha^i)+f(\alpha^j)=R_2 \end{aligned}\right\}$$

最简单的选取法是令 $f(\alpha^i)=\alpha^i$，此时有

$$\alpha^i+\alpha^j=R_1=R_2$$

显然无法由R_1和R_2解出 i 和 j。

其次命 $f(\alpha^i)=\alpha^{2i}$，有

$$\left.\begin{aligned} &\alpha^{i}+\alpha^{j}=R_1 \\ &\alpha^{2i}+\alpha^{2j}=(\alpha^{i}+\alpha^{j})^{2}=R_2 \end{aligned}\right\}$$

仍然无法解出 i 和 j。

若令 $f(\alpha^{i})=\alpha^{3i}$如何呢?这时得到

$$\left.\begin{aligned} &\alpha^{i}+\alpha^{j}=R_1 \\ &\alpha^{3i}+\alpha^{3j}=(\alpha^{i}+\alpha^{j})(\alpha^{2i}+\alpha^{i}\cdot\alpha^{j}+\alpha^{2j})=R_2 \end{aligned}\right\}$$

因此

$$R_1\cdot(R_1^2+\alpha^{i+j})=R_2$$

或

$$\alpha^{i+j}=\frac{R_2}{R_1}+R_1^2 \qquad (R_1\neq 0)$$

由此可见，α^{i} 和 α^{j} 是方程$(x+\alpha^{i})(x+\alpha^{j})=x^2+(\alpha^{i}+\alpha^{j})x+\alpha^{i+j}=x^2+R_1x+\left(\dfrac{R_2}{R_1}+R_1^2\right)$的根。于是只要能解 $GF(2^4)$ 上的 2 次方程，我们就可以由R_1和R_2解出α^{i}和α^{j}，从而得到 i 和 j。所以这种选取 f 的方案是可行的。

这样一来，H'形如

$$H'=\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{pmatrix}$$

注意，因为α^3是$\dfrac{15}{(3,15)}=5$阶域元素，故在第二行中，并非 α 的各次幂都出现。将H'写成$GF(2)$上矩阵的形式

$$H'=\begin{pmatrix} 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \\ 0&1&1&1&1&0&1&1&1&1&0&1&1&1&1 \\ 0&0&1&0&1&0&0&1&0&1&0&0&1&0&1 \\ 0&0&0&1&1&0&0&0&1&1&0&0&0&1&1 \\ 1&0&0&0&1&1&0&0&0&1&1&0&0&0&1 \end{pmatrix}$$

注意到，如果没有错误发生，则$R_1=R_2=0$；如果发生了一个错误，例如r_i出错，则$R_1=\alpha^i$，$R_2=\alpha^{3i}$。因此我们有如下的译码方案。

双纠错BCH码的译码方案 设$r=(r_0, r_1, \cdots, r_{n-1})$是接收向量，计算$r$的伴随式

$$\mathbf{s}^t=\begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

（1）若$R_1=R_2=0$，则判决没有出错；

（2）若$R_1\neq 0$，且$R_1=\alpha^i$，$R_2=R_1^3$，则判决第i位出错，并将r_i改为r_i+1；

（3）若$R_1\neq 0$，且$R_2\neq R_1^3$，解方程

$$x^2+R_1x+\left(\frac{R_2}{R_1}+R_1^2\right)=0$$

若该方程有根α^i和α^j，则判决第i和第j两位出错，并分别改正之；

（4）在其它情形，判决至少发生3个错误。

注意$GF(2^4)$上的2次方程在$GF(2^4)$中未必有根，故第（4）种情形是可能发生的。

顺便指出，解$GF(2^4)$中的2次方程不能使用常规的方法。一种解法是依次尝试域中的元素；另一种解法要用到所谓“迹”的概念，这里就不多说了。

例5.11.1 设接收向量r的第4和第11两位出错，则r的伴随式

$$\mathbf{s}^t=\begin{pmatrix} \alpha^4+\alpha^{11} \\ \alpha^{12}+\alpha^3 \end{pmatrix}=\begin{pmatrix} \alpha^{13} \\ \alpha^{10} \end{pmatrix}$$

即$R_1=\alpha^{13}$，$R_2=\alpha^{10}$。

因为

$$\frac{R_2}{R_1}+R_1^2=\alpha^{-3}+\alpha^{11}=\alpha^{12}+\alpha^{11}=1$$

故我们需解方程

$$x^2+\alpha^{13}x+1=0$$

解得两根为α^4和α^{11}。由此我们可以判定，r_4和r_{11}出错。

又如r的第 3 、 5 和 7 三位出错，则

$$\mathbf{s}^t=\begin{pmatrix}\alpha^3+\alpha^5+\alpha^7\\ \alpha^9+1+\alpha^6\end{pmatrix}=\begin{pmatrix}\alpha^8\\ \alpha^{10}\end{pmatrix}$$

因此 $R_1=\alpha^8$， $R_3=\alpha^{10}$， 并且$\frac{R_3}{R_1}+R_1^3=\alpha^2+\alpha=\alpha^5$。解方程

$$x^2+\alpha^8x+\alpha^5=0$$

依次试验 α 的各次幂，可知该方程无根，因此译码器检测出发生 3 个以上错误。

对于一般的双纠错BCH码，它的一致校验矩阵形如

$$\begin{pmatrix}1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2}\\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^m-2)}\end{pmatrix} \tag{5-32}$$

其中 α 是$GF(2^m)$ 中的本原域元素。它是二元（$n=2^m-1$， $n-2m$， d）码，其中 $d\geqslant 5$ 。

进一步的推广，以及对 t 一纠错BCH码的讨论，属于下一章的内容。

第六章　循环码理论的进一步发展

§6.1　循环码的零点

设 α 是 $GF(q)$ 的扩域上的一个 n 次单位原根。这里应当指出，如果 $(n, q)=1$，则包含 n 阶元素的 $GF(q)$ 的扩域一定存在。其实，求含有 n 阶元素的 $GF(q)$ 的最小扩域，相当于求最小的正整数 m，使

$$n \mid (q^m - 1),$$

此处 m 为 q 的模 n 阶。当 $(n, q)=1$ 时，这样的 m 必然存在。因为在模 n 运算下，序列

$$q, q^2, q^3, \cdots$$

中必然有相同者，例如

$$q^i \equiv q^j \quad (\bmod n), \quad i > j$$

于是由定理 3.2.6，

$$q^{i-j} \equiv 1 \quad (\bmod n) \qquad (6\text{-}1)$$

使式 (6-1) 成立的最小正整数 $i-j$ 即为所求的 m。再由定理 5.6.7，一定可以构造出阶为 q^m 的有限域 $GF(q^m)$，而在 $GF(q^m)$ 中就含有 n 阶元素。如果 $GF(q)$ 的特征为 p，则条件 $(n, q)=1$ 就等价于 $(n, p)=1$。

根据上述理由，在循环码的理论中，我们总是假定 $(n, q)=1$。特别在讨论二元循环码时，总假定 $(n, 2)=1$，即 n 永为奇数。

设 $x^n - 1 = f_1(x)f_2(x)\cdots f_k(x)$ 是 $x^n - 1$ 在 $GF(q)$ 上的既约因式分解。因为 $(n, q)=1$，故上述因式互不相同，即没有重因式。由此可见，码长为 n 的循环码共有 2^k 个。

我们规定，$\hat{f}_i(x)$ 表示除 $f_i(x)$ 外上述所有因式的乘积。例

如，$\hat{f}_1(x)=f_2(x)\cdots f_k(x)$。

定义 6.1.1 循环码 $\langle f_i(x)\rangle$ 称作**最大循环码**；循环码 $\langle \hat{f}_i(x)\rangle$ 称作**最小循环码**，或**既约循环码**。

上述定义来源于最小理想和最大理想的概念。

定义 6.1.2 称环R的理想I为R的**最小理想**，若R的理想N真包含于I，则$N=0$。称环R的理想$J\neq R$为R的**最大理想**，若J真包含于R的理想M，则$M=R$。

为方便计，本章令$R_n\triangleq GF(q)[x]/(x^n-1)$。由定理 4.6.2 易见，$\langle f_i(x)\rangle$ 是环 R_n 中的最大理想，故称为最大循环码。而 $\langle \hat{f}_i(x)\rangle$ 是环 R_n 中的最小理想，故称为最小循环码。后面我们将看到，在编码理论中，最小理想远比最大理想的概念重要。

设C为 (n,k) 循环码 $\langle g(x)\rangle$，$\deg g(x)=n-k$，并设α为n次单位原根，则有

$$g(x)=\prod_{i\in K}(x-\alpha^i),$$

其中K是分圆陪集的并集。我们有如下定义：

定义 6.1.3 称 n 次单位根 $\{\alpha^i|i\in K\}$ 为循环码 $C=\langle g(x)\rangle$的**零点**，亦即C的零点为其生成多项式的根。称其它的n次单位根，即 $h(x)=(x^n-1)/g(x)$ 的根为C的**非零点**。

下面的定理告诉我们，循环码可以用码字的公共零点来定义。

定理 6.1.1 设 $c(x)\in R_n$，则 $c(x)\in C=\langle g(x)\rangle$ 当且仅当

$$c(\alpha^i)=0,\quad i\in K$$

证明 若 $c(x)\in\langle g(x)\rangle$，则

$$c(x)=a(x)g(x)$$

其中 $\deg a(x)\leq k-1$。由于 $g(\alpha^i)=0$，$i\in K$，故有

$$c(\alpha^i)=a(\alpha^i)g(\alpha^i)=0,\quad i\in K。$$

反之，设 $c(\alpha^i)=0$，$i\in K$，则 $g(x)$的每一个根都是 $c(x)$ 的根，且因 $g(x)$ 无重根，故必有 $g(x)|c(x)$，因此 $c(x)\in\langle g(x)\rangle$。 （证毕）

对于具体的 $g(x)$，并不需要给出 $g(x)$ 的全部根。设 $g(x)$ 在 $GF(q)$ 上的既约分解式为

$$g(x)=f_{i_1}(x)f_{i_2}(x)\cdots f_{i_s}(x)$$

且设 β_{i_j} 是 $f_{i_j}(x)$ 的一个根，则

$c(\beta_i)=0 \quad (i=1,2,\cdots,n-k)$ 当且仅当

$$c(\beta_{i_j})=0 \quad (j=1,2,\cdots s)$$

事实上，$\{\beta_{i_1},\ \beta_{i_2},\cdots,\ \beta_{i_s}\}$ 是 $g(x)$ 的全部根，集合 $\{\beta_1,\beta_2,\cdots,\beta_{n-k}\}$ 的一个子集。因此当 $c(\beta_i)=0\ (i=1,2,\cdots,n-k)$ 时，自然有 $c(\beta_{i_j})=0\ (j=1,2,\cdots,p)$。反之若 $c(\beta_{i_j})=0\ (j=1,2,\cdots,s)$，则 $g(x)$ 的任意根 β_i 必为某一个 $f_{i_j}(x)$ 的根，从而 β_i 属于 β_{i_j} 的共轭元素系，故有 $c(\beta_i)=0$。

由定理 6.1.1

$c(x)\in\langle g(x)\rangle$，当且仅当 $c(\beta_{i_j})=0$

$$(j=1,2,\cdots,p)。$$

现在我们考虑仅需知道生成多项式 $g(x)$ 的一个根的情况。取 $q=2$，$n=2^m-1$，设 α 为 $GF(2^m)$ 上的本原域元素。于是 α 的最小多项式为

$$m^{(1)}(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^{2^2})\cdots(x-\alpha^{2^{m-1}})$$

它是一个 m 次本原多项式。由定理 5.5.4，$GF(2^m)$ 中的任意元素恒可表示为 $GF(2)$ 上次数低于 m 的 α 的多项式。

设 H 是一个 $m\times n$ 矩阵（$n=2^m-1$），它的第 j 列是 α^j 表示成次数低于 m 的 α 的多项式的系数

$$\alpha^j=\sum_{i=0}^{m-1}\varepsilon_{j_i}\alpha^i\leftrightarrow(\varepsilon_{j_0},\ \varepsilon_{j_1},\cdots,\varepsilon_{j_{m-1}}),$$

$$(j=0,1,\cdots,\ n-1)$$

即

$$H=(1\quad \alpha\quad \alpha^2\ \cdots\ \alpha^{m-1}\ \cdots\ \alpha^j\quad \cdots\ \alpha^{n-1})$$

$$=\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & \cdots & \varepsilon_{j_0} & \cdots \\ 0 & 1 & 0 & \cdots & 0 & \cdots & \varepsilon_{j_1} & \cdots \\ 0 & 0 & 1 & \cdots & 0 & \cdots & \varepsilon_{j_2} & \cdots \\ \vdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \cdots & \varepsilon_{j_{m-1}} & \cdots \end{pmatrix}$$

注意，这里我们按循环码的习惯表示方法，令

$$1\leftrightarrow\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix},\quad \alpha\leftrightarrow\begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix},\quad \cdots\alpha^{m-1}\leftrightarrow\begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}$$

与§5.11中的表示方法有所不同，在那里

$$1\leftrightarrow\begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix},\quad \alpha\leftrightarrow\begin{pmatrix}0\\\vdots\\1\\0\end{pmatrix},\quad \cdots\alpha^{m-1}\leftrightarrow\begin{pmatrix}1\\\vdots\\0\\0\end{pmatrix}$$

当然，两种表示法没有实质性的区别。

令 $c(x)=c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}$，则如上所述

$$c(x)\in\langle m^{(1)}(x)\rangle，当且仅当\ c(\alpha)=0$$

但是

$$c(\alpha)=c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}=(c_0\ \ c_1\ \cdots\ c_{n-1})\begin{pmatrix}1\\\alpha\\\alpha^2\\\vdots\\\alpha^{n-1}\end{pmatrix}$$

$$=cH'$$

其中 $c=(c_0,\ c_1,\cdots,c_{n-1})$。因此 $m\times n$ 矩阵 H 恰为由 $m^{(1)}(x)$ 生成的 $(n,\ n-m)$ 循环码的一致校验矩阵。由于矩阵 H 的各列可以表示为 $1,2,\cdots,2^m-1$ 的二进制数形式(经过适当的列置换)，因此我们得到了下述重要结果，

定理 6.1.2 设 $g(x)$ 为 $GF(2)$ 上的 m 次本原多项式，则二元 $(n=2^m-1,\ n-m)$ 循环码 $C=\langle g(x)\rangle$ 与二元 $(n,\ n-m)$ 汉明码等价。

例 6.1.1 设 α 为 $GF(2)$ 上 4 次本原多项式 $m^{(1)}(x)=x^4+x+1$ 的根，则由 $m^{(1)}(x)$ 所生成的 (15,11) 循环码的一致校验矩阵为

$$H=(1\ \ \alpha\ \ \alpha^2\ \ \alpha^3\ \ \alpha^4\ \ \alpha^5\ \ \alpha^6\ \ \alpha^7\ \ \alpha^8\ \ \alpha^9\ \ \alpha^{10}\ \ \alpha^{11}\ \ \alpha^{12}\ \ \alpha^{13}\ \ \alpha^{14})$$

$$=\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

上述循环码与 (15, 11) 汉明码等价。

编码时，编码器将信息序列 $(a_0, a_1, \cdots, a_{10})$ 变为

$$c(x)=a(x)(x^4+x+1)$$

其中

$$a(x)=a_0+a_1x+\cdots a_{10}x^{10}$$

译码时，若接收向量 $r(x)$ 包含一个错误，即

$$r(x)=c(x)+x^e$$

于是译码器计算伴随式为

$$rH^t=r(\alpha)=c(\alpha)+\alpha^e=\alpha^e$$

因此若伴随式为 α^e，则译码器判定第 e 个位置上有一个错误。

由此可见，将汉明码视为循环码时，译码手续与汉明码（作为线性码）一样简单，但编码器却比汉明码的情形简单得多，因为这时存储器只需存储生成多项式 $g(x)$。

例 6.1.2 设 $m^{(1)}(x)$ 的定义如前，考虑

$$g(x)=(x+1)m^{(1)}(x)$$

因为 $g(x)|(x^{15}-1)$，于是 (15, 10) 循环码 $\langle g(x)\rangle$ 的所有码字 $c(x)=c_0+c_1x+\cdots+c_{14}x^{14}$ 都有公共零点 1 和 α，即

$$c(1)=0,\qquad c(\alpha)=0$$

由于

$$c(1)=c_0+c_1+\cdots+c_{14}=(c_0c_1\cdots c_{14})\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix}$$

$$c(\alpha)=(c_0c_1\cdots c_{14})\begin{pmatrix}1\\\alpha\\\vdots\\\alpha^{14}\end{pmatrix}$$

因此

$$H=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\\hline 1&\alpha&\alpha^2&\alpha^3&\alpha^4&\alpha^5&\alpha^6&\alpha^7&\alpha^8&\alpha^9&\alpha^{10}&\alpha^{11}&\alpha^{12}&\alpha^{13}&\alpha^{14}\end{pmatrix}$$

$$=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\1&0&0&0&1&0&0&1&1&0&1&0&1&1&1\\0&1&0&0&1&1&0&1&0&1&1&1&1&0&0\\0&0&1&0&0&1&1&0&1&0&1&1&1&1&0\\0&0&0&1&0&0&1&1&0&1&0&1&1&1&1\end{pmatrix}$$

是由 $g(x)=(x+1)m^{(1)}(x)$ 生成的（15,10）循环码的一致校验矩阵，比（15,11）汉明码的一致校验矩阵多了一个全 1 行。这个（15,10）循环码是由（15,11）汉明码的偶重量码字组成的子汉明码，称为**增余删信汉明码**（增加一个多余度，减少一个信息位）。

对于 $GF(q)$ 的一般情形，类似于定理 6.1.2，我们有

定理 6.1.3 设 $n=\dfrac{q^m-1}{q-1}$，且 α 为 $GF(q^m)$ 中的 n 次单位原根。此外，设 $(m,q-1)=1$。于是，循环码

$$C\triangleq\{c(x)\,|\,c(\alpha)=0\}$$

与 q 元 $(n,n-m)$ 汉明码等价。

证明 由假设

$$
\begin{aligned}
n &= \frac{q^m - 1}{q - 1} = q^{m-1} + q^{m-2} + \cdots + q^2 + q + 1 \\
&= q^{m-1} + 2q^{m-2} + 3q^{m-3} + \cdots + (m-2)q^2 \\
&\quad + (m-1)q + 1 - q^{m-2} - 2q^{m-3} \\
&\quad - \cdots - (m-3)q^2 - (m-2)q \\
&= q\,(q^{m-2} + 2q^{m-3} + 3q^{m-4} + \cdots + (m-2)q \\
&\quad + (m-1)) + 1 - (q^{m-2} + 2q^{m-3} + 3q^{m-4} \\
&\quad + \cdots + (m-2)q + (m-1)) + (m-1) \\
&= (q-1)(q^{m-2} + 2q^{m-3} + \cdots + (m-2)q + m - 1) + m
\end{aligned}
$$

由此可得

$$(n, q-1) = (m, q-1) = 1$$

因此对于 $i = 1, 2, \cdots, n-1$，恒有

$$\alpha^{i(q-1)} \neq 1$$

假如不然，则有某个 j，使

$$\alpha^{j(q-1)} = 1$$

因此 $n \mid j(q-1)$。但是，$1 \leqslant j \leqslant n-1$，故 $n \nmid j$，所以 $(n, q-1) \neq 1$，与前边矛盾。

这样一来，我们断言

$$\alpha^i \overline{\in} GF(q), \quad i = 1, 2, \cdots, n-1$$

并且矩阵

$$H = (1\ \alpha\ \ \alpha^2 \cdots \alpha^{n-1})$$

中的任意两列在 $GF(q)$ 上都线性无关。如果

$$\alpha^i = \pi\alpha^j, \quad 0 \leqslant j < i < n-1$$

其中 $\pi \in GF(q)$，则

$$\alpha^{i(q-1)} = \alpha^{j(q-1)}$$

或

$$\alpha^{(i-j)(q-1)} = 1$$

与前边矛盾。根据定义 2.6.2，我们知道 H 是 q 元 $(n, n-m)$ 汉明码的一致校验矩阵。（证毕）

例6.1.3 我们有

$$x^8-1=Q^{(1)}(x)Q^{(2)}(x)Q^{(4)}(x)Q^{(8)}(x)$$
$$=(x-1)(x+1)(x^2+1)(x^4+1)$$

在 $GF(3)$ 上

$$x^4+1=(x^2+x+2)(x^2+2x+2)$$

由此可见

$$x^2+x+2,\qquad x^2+2x+2$$

是 $GF(3)$ 上的两个2次本原多项式。

表6-1给出了由 $\alpha^2+\alpha+2=0$ 定义的 $GF(3^2)$ 的一种形式，另一种同构的形式可由本原多项式 x^2+2x+2 给出。

表 6-1

α 的 幂	$GF(3)$ 上 α 的多项式	
	1	α
1	1	0
α	0	1
α^2	1	2
α^3	2	2
α^4	2	0
α^5	0	2
α^6	2	1
α^7	1	1

设 β 是 $GF(3^2)$ 中的4次单位原根，即

$$\beta=\alpha^2\qquad(\text{或 } \beta=\alpha^3)$$

于是循环码

$$C=\{c(x)\,|\,c(\beta)=0\}$$

的一致校验矩阵为

$$H=(1\quad\beta\quad\beta^2\quad\beta^3)$$
$$=(1\quad\alpha^2\quad\alpha^4\quad\alpha^6)$$
$$=\begin{pmatrix}1&1&2&2\\0&2&0&1\end{pmatrix}$$

显然 C 不是三元 $(4,2)$ 汉明码。

由于

$$(x-\alpha^2)(x-\alpha^6)=x^2+1$$

是 C 的生成多项式，可见 C 的生成矩阵为

$$G=\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

我们不可能使三元（4，2）循环码与三元（4，2）汉明码等价，因此在等价的意义上，三元（4，2）汉明码不是循环码。

下面扩展循环码的定义。如果对任意码字 $(c_0, c_1, \cdots, c_{n-1}) \in C$，恒有

$$(-c_{n-1},\ c_0, c_1, \cdots, c_{n-2}) \in C,$$

则称 C 为**负循环码**。

类似于循环码，我们可以平行地建立一套关于负循环码的理论，诸如生成多项式，校验多项式等，但是负循环码的生成多项式 $g(x)$ 与校验多项式 $h(x)$ 之间满足关系

$$x^n+1=g(x)h(x)$$

例如在 $GF(3)$ 上，因为

$$x^4+1=(x^2+x+2)(x^2+2x+2)$$

所以三元（4，2）负循环码 $C=\langle g(x)\rangle=\langle x^2+x+2\rangle$ 的生成矩阵为

$$G=\begin{pmatrix} 2 & 1 & 1 & 0 \\ 0 & 2 & 1 & 1 \end{pmatrix}$$

又因为

$$\tilde{h}(x)=2x^2+2x+1$$

故 C 的一致校验矩阵为

$$H=\begin{pmatrix} 1 & 2 & 2 & 0 \\ 0 & 1 & 2 & 2 \end{pmatrix}$$

由此可见，C 是三元（4，2）汉明码。

因此三元（4，2）汉明码是负循环码（在等价的意义上）。

§6.2 由循环码的零点构造循环码

设 $g(x)$ 为 (n, k) 循环码 C 的生成多项式，且 $\{\alpha^i | i \in K\}$ 是循环码 C 的全部零点，则由定理 6.1.1，

$$c(x)\in C \quad 当且仅当 c(\alpha^i)=0,\quad i\in K$$

令 $m^{(i)}(x)$ 为 α^i 的最小多项式（$i\in K$），则 $m^{(i)}(x)|g(x)$，从而

$$[m^{(i)}(x)|\ i\in K]\,|\,g(x)$$

其中 $[m^{(i)}(x)|\ i\in K]$ 表示 $\{m^{(i)}(x)|\ i\in K\}$ 的最低公倍式。另一方面，因 $g(x)$ 没有重根，且 $g(x)$ 的每一个根皆为 $[m^{(i)}(x)|\ i\in K]$ 的根，故

$$g(x)\,|\,[m^{(i)}(x)|\ i\in K]$$

于是

$$g(x)=[m^{(i)}(x)|\ i\in K] \tag{6-2}$$

因此在已知生成多项式的全部根（即已知循环码的全部零点）时，可以通过求出每个根的最小多项式再求出它们的最低公倍式的方法来找出生成多项式 $g(x)$。求最小多项式时，可采用 § 5.9 中所介绍的办法。

其次，我们还可以根据循环码的全部零点来决定循环码的最小码长 n。事实上，码长 n 即为满足 $g(x)|(x^n-1)$ 的最小正整数 n，亦即 $g(x)$ 的周期 $p(g)$。若设 $g(x)$ 在 $GF(q)$ 上的既约分解式为

$$g(x)=f_{i_1}(x)f_{i_2}(x)\cdots f_{i_t}(x)$$

则由推论 5.10.3.1，有

$$n=p(g)=[p(f_{i_1}),\ p(f_{i_2})\cdots,\ p(f_{i_t})] \tag{6-3}$$

又因每一个既约多项式 $f_{i_j}(x)$ 的周期即为 $f_{i_j}(x)$ 的根的阶，故有

$$n=[e^i|\ i\in K]$$

其中 α^i 之阶为 $e^i(i\in K)$。

例6.2.1 设 α 为 $GF(2)$ 上 4 次本原多项式 x^4+x+1 的根。设已知循环码 C 的全部零点为

$$\{\alpha^i|\ i\in K\}$$

其中

$$K=\{1, 2, 3, 4, 5, 6\}$$
$$=C_1\cup C_3\cup C_5$$

因此，C的生成多项式为

$$g(x)=m^{(1)}(x)m^{(3)}(x)m^{(5)}(x)$$
$$=(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)$$
$$=x^{10}+x^8+x^5+x^4+x^2+x+1$$

并且C的最小码长应为

$$n=[15, 5, 3]=15$$

因此$C=\langle g(x)\rangle$是（15, 5）循环码，它的一致校验矩阵为

$$H=\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \\ 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} & 1 & \alpha^5 & \alpha^{10} \end{pmatrix}$$

$$=\left(\begin{array}{ccccccccccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

请读者注意，由于$\deg g(x)=10$，故H矩阵的秩应当为 10，因此上述矩阵的最后两行可以去掉（最后一行为全零行，而第 11 行与第 10 行完全相同）。

例 6.2.2 考虑$q=2$，$n=9$时的情形。因为

$$c_0=\{0\}$$
$$c_1=\{1, 2, 4, 8, 7, 5\}$$
$$c_3=\{3, 6\}$$

而且 2 的模 9 阶为 6，即包含 9 次单位原根的 $GF(2)$ 的最小扩域为 $GF(2^6)$。此外

$$
\begin{aligned}
x^9-1&=Q^{(1)}(x)Q^{(3)}(x)Q^{(9)}(x)\\
&=(x-1)(x^2+x+1)(x^6+x^3+1)\\
&=m^{(0)}(x)m^{(3)}(x)m^{(1)}(x)
\end{aligned}
$$

最大循环码$\langle m^{(1)}(x)\rangle=\langle x^6-x^3+1\rangle$的$H$矩阵中，任意两列彼此不同，故该码的最小距离 $d\geqslant 3$。又因

$$(1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0)$$

是其中一个码字，故有 $d=3$。因此，这是一个$(9,3,3)$码。

最小循环码$\langle \bar{m}^{(1)}(x)\rangle=\langle m^{(0)}(x)m^{(3)}(x)\rangle=\langle x^3+1\rangle$是$(9,6,2)$码，因为它有一个码字

$$(1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0)$$

设 α 是 $GF(2)$ 上 6 次本原多项式 x^6+x+1 的根，则 $\beta=\alpha^7$ 是$GF(2^6)$ 中的 9 次单位原根。在由 $\alpha^6+\alpha+1=0$ 定义的域 $GF(2^6)$ 中

$$
\begin{aligned}
1\quad &\leftrightarrow (1\quad 0\quad 0\quad 0\quad 0\quad 0)\\
\beta^3=\alpha^{21}\ &\leftrightarrow (1\quad 1\quad 0\quad 1\quad 1\quad 1)\\
\beta^6=\alpha^{42}\ &\leftrightarrow (0\quad 1\quad 0\quad 1\quad 1\quad 1)
\end{aligned}
$$

故该码的H矩阵为

$$
H=\left(\begin{array}{ccccccccc}
1&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0\\
\hline
1&1&0&1&1&0&1&1&0\\
0&1&1&0&1&1&0&1&1\\
0&0&0&0&0&0&0&0&0\\
0&1&1&0&1&1&0&1&1\\
0&1&1&0&1&1&0&1&1\\
0&1&1&0&1&1&0&1&1
\end{array}\right)
$$

实际上，H矩阵的秩为 3，故去掉其中线性相关的行之后

$$H=\begin{pmatrix}1&1&1&1&1&1&1&1&1\\1&1&0&1&1&0&1&1&0\\0&1&1&0&1&1&0&1&1\end{pmatrix}$$

我们再作一个注记。由这个码的校验多项式

$$h(x)=1+x^3+x^6=\tilde{h}(x)$$

可以直接得出另一种形式的一致校验矩阵

$$H'=\begin{pmatrix}1&0&0&1&0&0&1&0&0\\0&1&0&0&1&0&0&1&0\\0&0&1&0&0&1&0&0&1\end{pmatrix}$$

§6.3 幂 等 元

迄今为止，我们将循环码的生成多项式视为码中次数最低的首一多项式 $g(x)$。下面的引理告诉我们，其它的多项式也可以生成循环码$\langle g(x)\rangle$。

引理 6.3.1 设$C=\langle g(x)\rangle$的零点集合为$\{\alpha^i \mid i\in K\}$，若$p(x)\in R_n$不引入新的零点，即对一切 $i\notin K$，恒有

$$p(\alpha^i)\neq 0$$

则$g(x)$ 和$p(x)g(x)$ 生成同一个循环码，即

$$C=\langle g(x)\rangle=\langle p(x)g(x)\rangle$$

证明 由于$g(x)\mid p(x)g(x)$，故根据定理4.6.2，$\langle p(x)g(x)\rangle\subseteq\langle g(x)\rangle$。设$x^n-1=g(x)h(x)$，则条件$p(\alpha^i)\neq 0$ $(i\notin K)$ 等价于 $(p(x), h(x))=1$。因此由定理 3.1.4，存在多项式$a(x)$ 和$b(x)$，使得

$$1=a(x)p(x)+b(x)h(x)$$

因此

$$g(x)=a(x)p(x)g(x)+b(x)g(x)h(x)$$

但在 R_n 中，$g(x)h(x)=0$，故有

$$g(x)=a(x)p(x)g(x)$$

因此

$$\langle g(x)\rangle \subseteq \langle p(x)g(x)\rangle$$

于是

$$\langle g(x)\rangle = \langle p(x)g(x)\rangle$$

（证毕）

由此可见$\langle g(x)\rangle = \langle g^2(x)\rangle$。

引理6.3.2 设$\xi \in GF(q^m)$，且ξ是n次单位根，即$\xi^n = 1$，则

$$\sum_{i=0}^{n-1} \xi^i = \begin{cases} 0, & 若\ \xi \neq 1 \\ n, & 若\ \xi = 1 \end{cases}$$

证明 当$\xi = 1$时，

$$\sum_{i=0}^{n-1} \xi^i = \sum_{i=0}^{n-1} 1 = n$$

当$\xi \neq 1$时

$$\sum_{i=0}^{n-1} \xi^i = \frac{\xi^n - 1}{\xi - 1} = 0$$

（证毕）

引理6.3.3（反转公式）设α为n次单位原根，且$c(x) = c_0 + c_1 x + \cdots + c_n x^{n-1}$。于是，$c(x)$的系数可由下式确定：

$$c_i = \frac{1}{n} \sum_{j=0}^{n-1} c(\alpha^j)\alpha^{-ij} \quad 0 \leqslant i \leqslant n-1 \qquad (6\text{-}4)$$

证明 因为

$$\sum_{j=0}^{n-1} c(\alpha^j)\alpha^{-ij} = \sum_{j=0}^{n-1}\left(\sum_{k=0}^{n-1} c_k \alpha^{jk}\right)\alpha^{-ij}$$

$$= \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} c_k \alpha^{j(k-i)} = \sum_{k=0}^{n-1} c_k \sum_{j=0}^{n-1} \alpha^{j(k-i)}$$

故由引理6.3.2，

$$\sum_{j=0}^{n-1} \alpha^{j(k-i)} = \begin{cases} 0, & 若\ k \neq i \\ n, & 若\ k = i \end{cases}$$

因此

$$\sum_{j=0}^{n-1} c\ (\alpha^{j})\alpha^{-ij} = n\,c_i$$

（证毕）

特别，当所讨论的是特征为2的域时，因为n总是奇数，故$n = 1$。因此有

推论 6.3.3.1 设α为$GF(2^m)$中的n次单位原根，则式(6-4)变为

$$c_i = \sum_{j=0}^{n-1} c\ (\alpha^{j})\alpha^{-ij},\quad 0 \leqslant i \leqslant n-1 \qquad (6\text{-}5)$$

既然作为理想的循环码可以有不只一个生成元，那么，我们为什么偏重于生成多项式呢？因为由它可以立即确定循环码的维数。但是求生成多项式必须将$x^n - 1$分解因式，而n很大时，这是一件十分困难的任务。下面我们介绍的幂等生成元可以不必分解$x^n - 1$而求得，是循环码的另一类重要的生成元。

为论述方便起见，我们仅讨论二元循环码，其中n为奇数。α是某个n次单位原根。

定义 6.3.1 设$e(x) \in R_n$，如果

$$e^2(x) = e(x)$$

则称$e(x)$为**幂等元**。

例如，$e(x) \in R_7$。设$e(x) = e_0 + e_1 x + \cdots + e_6 x^6$，则$e^2(x) = e_0 + e_1 x^2 + \cdots + e_6 x^5$。显然$e^2(x) = e(x)$，当且仅当$e_i = e_{2i} (\mathrm{mod}\ 7)$。因此幂等元的非零项的方幂集合是一个分圆陪集的并集。当$n = 7$时，我们有

$$C_0 = \{0\},\ C_1 = \{1, 2, 4\},\ C_3 = \{3, 6, 5\}$$

所以1，$x + x^2 + x^4$，$1 + x^3 + x^6 + x^5$等等都是R_7中的幂等元。

类似地，我们可以证明一般情形。

引理 6.3.4 $e(x) = \sum_{i=0}^{n-1} e_i x^i \in R_n$是幂等元，当且仅当

$$e_i = e_{2i}\ (\mathrm{mod}\ n)$$

当且仅当 $e(x)$ 的非零项的方幂集合是一个分圆陪集的并集。

很明显，1恒为幂等元，因而 $e(x)$ 是幂等元，当且仅当 $1+e(x)$ 是幂等元。

定义 6.3.2 能生成循环码 C 的幂等元 $e(x)$ 称为**幂等生成元**。记作 $C=\langle e(x)\rangle$。

读者应注意下述符号的区别：$C=\langle g(x)\rangle$ 表示 C 的生成元 $g(x)$ 为生成多项式；$C=\langle e(x)\rangle$ 表示 C 的幂等生成元为 $e(x)$；如不特别注明，一般是 $C=\langle p(x)\rangle$ 表示 $p(x)$ 为 C 的其它类型的生成元等等。

幂等生成元有下述重要特征性质：

引理 6.3.5 $c(x)\in C$ 当且仅当

$$c(x)e(x)=c(x)$$

亦即幂等生成元 $e(x)$ 是 C 中的单位元。

证明 若 $c(x)=c(x)e(x)$，显然 $c(x)\in C=\langle e(x)\rangle$。反之，若 $c(x)\in C=\langle e(x)\rangle$，则

$$c(x)=b(x)e(x)$$

于是

$$c(x)e(x)=b(x)e^2(x)=b(x)e(x)=c(x)$$

（证毕）

一个循环码可以有若干个幂等元，但是幂等生成元只有一个，如下述定理所示：

定理 6.3.1 循环码 $C=\langle g(x)\rangle$ 有且仅有一个幂等生成元 $e(x)=p(x)g(x)$，并且

$$e(\alpha^i)=0 \text{ 当且仅当 } g(\alpha^i)=0$$

其中 α 为 $GF(2)$ 的某个扩域上的 n 次单位原根。

证明 设 $x^n+1=g(x)h(x)$。根据我们对 n 的假设（即 n 为奇数），x^n+1 没有重因式，故 $(g(x),h(x))=1$。由定理 3.1.4，存在多项式 $p(x)$，$q(x)$，使得

$$p(x)g(x)+q(x)h(x)=1 \tag{6-6}$$

令 $e(x)=p(x)g(x)$，则 $e(x)\in C=\langle g(x)\rangle$。将式(6-6)

两边同乘 $p(x)g(x)$，有

$$p(x)g(x)(p(x)g(x)+q(x)h(x))=p(x)g(x)$$

则在 R_n 中，上式变为

$$e^2(x)+0=e(x)$$

即 $e(x)$ 是幂等元。

设 ξ 是任意 n 次单位根．则因 $(g(x),\ h(x))=1$，故 ξ 或为 $g(x)$ 的根；或为 $h(x)$ 的根；但不能同时为 $g(x)$ 和 $h(x)$ 的根。由（6-6）可见，$(p(x),\ h(x))=1$，于是 $h(\xi)\neq 0$ 当且仅当 $p(\xi)=0$ 当且仅当 $g(\xi)=0$。因此 $p(x)$ 并不引入新的零点。由引理 6.3.1，有

$$\langle p(x)g(x)\rangle=\langle e(x)\rangle=\langle g(x)\rangle=C$$

亦即 $e(x)$ 是幂等生成元。

假定 C 还有一个幂等生成元 $f(x)$，则由引理 6.3.5，得

$$f(x)e(x)=e(x)=f(x)$$

故 C 的幂等生成元仅有一个。（证毕）

式（6-6）告诉我们已知生成多项式时求幂等生成元的方法。

例如，(7, 4, 3) 汉明码 C 的生成多项式为 $g(x)=x^3+x+1$，则 $h(x)=(x+1)(x^3+x^2+1)=x^4+x^2+x+1$，并且

$$xg(x)+h(x)=1$$

因此 C 的幂等生成元为

$$e(x)=xg(x)=x^4+x^2+x$$

当然我们可以通过欧几里德算法求出式(6-6)，从而由 $g(x)$ 和 $h(x)$ 确定 $e(x)$，但往往比较麻烦。下面的方法是直接得到式（6-6）的一条捷径。

设 $x^n+1=g(x)h(x)$，两边同时求（形式）导数后得

$$x^{n-1}=g'(x)h(x)+g(x)h'(x)$$

因此

$$x^n=xg'(x)h(x)+xg(x)h'(x)$$

于是在 R_n 中，有

$$1=xg'(x)h(x)+xh'(x)g(x)$$

由此可见，幂等生成元为

$$e(x)=x\,h'(x)\,g(x) \tag{6-7}$$

设 $h(x)=h_0(x)+h_1(x)$，其中 $h_0(x)$ 和 $h_1(x)$ 分别由 $h(x)$ 中的偶次方幂项和奇次方幂项组成，于是 $h_0'(x)=0$，$x\,h_1'(x)=h_1(x)$，故

$$x\,h'(x)=x\,h_1'(x)=h_1(x)$$

因此

$$e(x)=h_1(x)\,g(x) \tag{6-8}$$

即幂等生成元是 $g(x)$ 与 $\frac{x^n+1}{g(x)}$ 中的奇次方幂项的乘积。

在上例中，$h(x)=x^4+x^2+x+1$，故 $h_1(x)=x$，因此

$$e(x)=x\,g(x)=x^4+x^2+x$$

注意当 $\deg h(x)$ 为奇数时，$x\,h'(x)\,g(x)=h_1(x)\,g(x)$ 为 n 次多项式，而在 R_n 中 $x^n=1$，故当且仅当 $\deg h(x)$ 为奇数时，$e(x)$ 中含有 1。上述事实可以用于验证所得的结果。

此外，当 $h(x)\neq 1$ 时（$h(x)=1$ 对应于 $g(x)=x^n+1$ 的平凡情形），$h(x)$ 中一定含有奇次方幂项，否则 $h(x)$ 是某一个多项式的平方，与 n 为奇数的假设矛盾。

反过来，如果知道循环码 C 的幂等生成元，为了求 C 的维数等原因，我们往往希望求 C 的生成多项式。下述定理解决了这一问题。

定理 6.3.2 设 $e(x)$ 为 C 的幂等生成元，则 C 的生成多项式为

$$g(x)=(e(x),\ x^n+1)$$

证明 由定理 6.3.1 的证明中可知，$e(x)=p(x)\,g(x)$，其中 $(p(x),\ h(x))=1$。因此由定理 3.1.6，我们有

$$\begin{aligned}(e(x),\ x^n+1)&=(p(x)\,g(x),\ g(x)\,h(x))\\&=g(x)(p(x),\ h(x))\\&=g(x)\end{aligned}$$

（证毕）

通过分圆陪集可以容易地求出所有可能的幂等元，从而不必分解 x^n+1 就能生成全部码长为 n 的二元循环码。不仅如此，幂等元的重要性还体现在许多重要的编码定理的证明都涉及到幂等元，这里就不多讲了。

类似于定理 4.6.4 和定理 4.6.5，我们有下述结果。

定理6.3.3 设 $C_1=\langle e_1(x)\rangle$ 且 $C_2=\langle e_2(x)\rangle$，则 $C_1\cap C_2=\langle e_1(x)e_2(x)\rangle$，$C_1+C_2=\langle e_1(x)+e_2(x)+e_1(x)e_2(x)\rangle$

证明 显然 $e_1(x)e_2(x)\in C_1\cap C_2$。因为

$$(e_1(x)e_2(x))^2=e_1^2(x)e_2^2(x)=e_1(x)e_2(x)$$

故 $e_1(x)e_2(x)$ 是 $C_1\cap C_2$ 中的幂等元。任取 $c(x)\in C_1\cap C_2$，则

$$c(x)e_1(x)e_2(x)=c(x)e_2(x)=c(x)$$

故 $e_1(x)e_2(x)$ 是 $C_1\cap C_2$ 中的单位元。由引理 6.3.5，$e_1(x)e_2(x)$ 是 $C_1\cap C_2$ 中的幂等生成元。

$e_1(x)+e_2(x)+e_1(x)e_2(x)\in C_1+C_2$，且 $(e_1(x)+e_2(x)+e_1(x)e_2(x))^2=e_1^2(x)+e_2^2(x)+e_1^2(x)e_2^2(x)=e_1(x)+e_2(x)+e_1(x)e_2(x)$，因此 $e_1(x)+e_2(x)+e_1(x)e_2(x)$ 是 C_1+C_2 中的幂等元。任取 $c(x)\in C_1+C_2$，则 $c(x)=c_1(x)+c_2(x)$，其中 $c_1(x)\in C_1$，$c_2(x)\in C_2$。因此，

$$\begin{aligned}&(c_1(x)+c_2(x))(e_1(x)+e_2(x)+e_1(x)e_2(x))\\&=c_1(x)e_1(x)+c_1(x)e_2(x)+c_1(x)e_1(x)e_2(x)\\&+c_2(x)e_1(x)+c_2(x)e_2(x)+c_2(x)e_1(x)e_2(x)\\&=c_1(x)+c_1(x)e_2(x)+c_1(x)e_2(x)\\&+c_2(x)e_1(x)+c_2(x)+c_2(x)e_1(x)\\&=c_1(x)+c_2(x)\end{aligned}$$

即 $e_1(x)+e_2(x)+e_1(x)e_2(x)$ 是 C_1+C_2 中的单位元。于是 $C_1+C_2=\langle e_1(x)+e_2(x)+e_1(x)e_2(x)\rangle$。 〈证毕〉

引理6.3.6 $e(x)$ 是幂等元，当且仅当

$$e(\alpha^i)=0\text{ 或 }1,\quad i=0,1,\cdots,n-1$$

证明 设 $e(x)$ 为幂等元，则 $e^2(\alpha^i)=e(\alpha^i)$，故由定理 5.4.6，$e(\alpha^i)=0$ 或 1。

反之，令 $e(x)=\sum_{i=0}^{n-1} e_i x^i$，由引理6.3.3，得

$$e_i=\sum_{j=0}^{n-1} e(\alpha^j)\alpha^{-ij}$$

因为 $e(\alpha^j)=0$ 或1，故

$$e_i=\sum_{s}\sum_{j\in C_s}\alpha^{-ij}$$

其中 s 遍历具有下述性质的分圆陪集：$\{C_s|\ e(\alpha^j)=1,\ j\in C_s\}$。所以 $e_i=e_{2i}(\bmod\ n)$，即 $e(x)$为幂等元(引理6.3.4)。〈证毕〉

由上述引理即得

引理6.3.7 $C=\langle g(x)\rangle=\langle e(x)\rangle$ 的维数等于使 $g(\alpha^i)\neq 0$ 的 α^i $(0\leqslant i\leqslant n-1)$ 的个数，也等于使 $e(\alpha^i)=1$ 的 α^i 的数目。

证明 由定理6.3.1及引理6.3.6，$g(\alpha^i)\neq 0$，当且仅当 $e(\alpha^i)\neq 0$，当且仅当 $e(\alpha^i)=1$。〈证毕〉

设 $a(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}$，定义 $a^*(x)$ 为

$$a^*(x)\triangleq a_0+a_{n-1}x+\cdots+a_1x^{n-1}$$

即常数项不变，其它系数倒排。显然有

$$\begin{aligned}a(\alpha^{-1})&=a_0+a_1\alpha^{-1}+\cdots+a_{n-1}\alpha^{-(n-1)}\\&=\alpha^n(a_0+a_1\alpha^{-1}+\cdots+a_{n-1}\alpha^{-(n-1)})\\&=a_0+a_{n-1}\alpha+\cdots+a_1\alpha^{n-1}\\&=a^*(\alpha)\end{aligned}$$

引理6.3.8 $e(x)$ 是幂等元，当且仅当 $e^*(x)$是幂等元。

证明 设 $e(x)$ 为幂等元，则

$$e(x)=\sum_{s}\sum_{j\in C_s}x^j$$

于是

$$e^*(x)=\sum_{s}\sum_{j\in C_s}x^{-j}=\sum_{s}\sum_{j\in C_{-s}}x^j$$

即 $e^*(x)$ 也是幂等元。又因 $e^{**}(x)=e(x)$，故反之亦真。

〈证毕〉

定理6.3.4 设 $C=\langle e(x)\rangle$，则

$$C^{\perp}=\langle(1+e(x))^*\rangle$$

证明 设 α_1，…，α_n 为 n 次单位根，其中 $\alpha_i\neq\alpha_j$，$i\neq j$。假定 α_1，…，α_k 为 C 的零点，即 $e(\alpha_i)=0$，$1\leqslant i\leqslant k$，$e(\alpha_i)=1$，$k+1\leqslant i\leqslant n$。于是 $1+e(x)$ 的零点为 α_{k+1}，…，α_n，而 $(1+e(x))^*$ 的零点为 α_{k+1}^{-1}，…，α_n^{-1}。由定理4.6.1，它们都是 $C^{\perp}$ 的零点。因此 $(1+e(x))^*$ 生成 $C^{\perp}$。再由引理6.3.8，$(1+e(x))^*$ 是幂等元。〈证毕〉

从定理6.3.4的证明中即得

推论6.3.4.1 设 $x^n+1=g(x)h(x)$，且 $C=\langle g(x)\rangle=\langle e(x)\rangle$，则

$$\langle h(x)\rangle=\langle 1+e(x)\rangle$$

即以 $h(x)$ 为生成多项式的循环码的幂等生成元为 $1+e(x)$。

值得注意的是，对于一般的幂等元，定理6.3.4未必成立，即若 $e(x)$ 为 C 的幂等元，$(1+e(x))^*$ 未必是 $C^{\perp}$ 的幂等元。

§6.4 本原幂等元

本节仍局限于讨论二元循环码，其中码长 n 为奇数，设 α 为 $GF(2)$ 的某个扩域上的 n 次单位原根。

定义6.4.1 最小循环码的幂等生成元称为**本原幂等元**。

如所周知，最小循环码的非零点集合形如

$$\{\alpha^i \mid i\in C_s\}$$

通常的记法是，将这一最小循环码记为 μ_s，它的本原幂等元记为 θ_s，亦即 $\mu_s=\langle\theta_s\rangle$。因此，我们有

$$\theta_s(\alpha^j)=\begin{cases}1, & 若\ j\in C_s\\ 0, & 其它情形\end{cases}\tag{6-9}$$

当 $s=0$ 时，μ_0 的校验多项式为 $x+1$，因此 μ_0 唯一的非

零点是 $\alpha^0=1$。显然有

$$\theta_0(x)=\frac{x^n+1}{x+1}=\sum_{i=0}^{n-1}x^i$$

对于一般的 s，我们有

定理6.4.1

$$\theta_s(x)=\sum_{i=0}^{n-1}e_ix^i$$

其中

$$e_i=\sum_{j\in C_s}\alpha^{-ij},\quad i\geqslant 0$$

证明 由引理6.3.3的推论和式（6-9）有

$$e_i=\sum_{j=0}^{n-1}\theta_s(\alpha^j)\alpha^{-ij}=\sum_{j\in C_s}\alpha^{-ij}$$

〈证毕〉

本原幂等元有下述重要性质。

定理6.4.2

（1）若 $i\neq j$，则 $\theta_i\theta_j=0$

（2）$\sum_s\theta_s=1$

（3）R_n 是 μ_s 的直和，即任意 $a(x)\in R_n$ 都可以唯一地表示成

$$a(x)=\sum_s a_s(x)$$

其中 $a_s(x)\in\mu_s=\langle\theta_s\rangle$

（4）$e(x)$ 是幂等元当且仅当

$$e(x)=\sum_s a_s\theta_s$$

其中 $a_s=0$ 或 1。

证明

（1） 当 $i \neq j$ 时，$\mu_i = \langle \theta_i \rangle$ 和 $\mu_j = \langle \theta_j \rangle$ 是不同的最小理想。由于理想 $\mu_i \cap \mu_j$ 真包含于 μ_i，故 $\mu_i \cap \mu_j = 0$。而 $\theta_i \theta_j \in \mu_i \cap \mu_j$，因此 $\theta_i \theta_j = 0$。

（2） 由定理 6.4.1，有

$$\sum_s \theta_s = \sum_s \sum_{i=0}^{n-1} \left(\sum_{j \in C_s} \alpha^{-ij} \right) x^i$$
$$= \sum_{i=0}^{n-1} x^i \left(\sum_s \sum_{j \in C_s} \alpha^{-ij} \right)$$
$$= \sum_{i=0}^{n-1} x^i \sum_{j=0}^{n-1} \alpha^{-ij}$$

再由引理 6.3.2，得

$$\sum_s \theta_s = n = 1$$

（3） 由上面的结果，对任意 $a(x) \in R_n$ 恒有

$$a(x) = a(x) \sum_s \theta_s(x)$$
$$= \sum_s a(x) \theta_s(x)$$
$$= \sum_s a_s(x)$$

其中 $a_s(x) \in \mu_s = \langle \theta_s \rangle$。

（4） 设 $e(x)$ 为幂等元，则 $e(x)$ 的非零点是本原幂等元的非零点集合的并集。根据引理 6.3.6 和式（6-9），有

$$e(x) = \sum_s a_s \theta_s, \quad a_s \in GF(2)$$

反之显然。 〈证毕〉

由 $\theta_s(\alpha^{-1}) = \theta_s^*(\alpha)$ 可知，

$$\theta_s^*(\alpha^j)=\begin{cases}1, & 若\ j\in C_{-s}\\ 0, & 其它情形\end{cases}$$

故 $\theta_s^*(x)$ 也是本原幂等元，因此存在一个最小的正整数 s'，使得

$$\theta_s^*(x)=\theta_{s'}(x)$$

其中 $s'\in C_{-s}$。

最后我们介绍关于最小理想的结构定理。

定理6.4.3 最小理想 $\mu_s=\langle\theta_s\rangle$ 是一个域。若 μ_s 的维数为 m，则 μ_s 与 $GF(2^m)$ 同构。

证明 设 $c(x)\neq 0\in\mu_s$，则 $\langle c(x)\rangle$ 是 μ_s 中的一个非零理想。由于 μ_s 是最小理想，故 $\langle c(x)\rangle=\mu_s$。因此

$$\theta_s=a(x)c(x)$$

其中 $a(x)\in R_n$。若 $a(x)\in\mu_s$，则 $a(x)$ 即为 $c(x)$ 之逆。无论如何，$a(x)\theta_s(x)\in\mu_s$，因而是 $c(x)$ 之逆。所以 μ_s 是一个域。

若 μ_s 的维数为 m，则 μ_s 中有 2^m 个元素。μ_s 的生成多项式是 m 次既约多项式，故可用于构造 $GF(2^m)$，在同构的意义上，具有 2^m 个元素的域只有一个。 〈证毕〉

在结束本节之前，我们作一个注记。类似地可以定义 $GF(q)$ 上的循环码的幂等元，并建立一系列相应的引理和定理。例如，$C=\langle e(x)\rangle$，则 $C^{\perp}=\langle(1-e(x))^*\rangle$。又如 m 维的最小理想 $\mu_s=\langle\theta_s\rangle$ 与 $GF(q^m)$ 同构，等等。

§6.5 例

为了消化前面所讲的关于循环码的一般性质，这一节我们举两个例子。

例6.5.1 考虑 $n=7$ 时的全体二元循环码。

因为 $x^7+1=(x+1)(x^3+x+1)(x^3+x^2+1)$

故码长为 7 的二元循环码共有 $2^3=8$ 个。我们不考虑以下两种平

凡情形：其一是整个空间，其幂等生成元为1；其二是零向量，它的幂等生成元为0。

设α为$GF(2)$上3次本原多项式x^3+x+1的根。$n=7$时的分圆陪集为

$$C_0=\{0\},\ C_1=\{1,\ 2,\ 4\},\ C_3=\{3,\ 6,\ 5\}$$

由此可得到全部8个幂等元。表6-2中列出了6个码的维数、生成多项式和幂等生成元。

由表6-2，读者不难验证前面所讲的诸项结果。

表 6-2

码	维数	生成多项式	幂等生成元
C_1	1	$g_1(x)=(x^3+x+1)(x^3+x^2+1)$	$\theta_0=1+x+x^2+x^3+x^4+x^5+x^6$
C_2	3	$g_2(x)=(x+1)(x^3+x^2+1)$	$\theta_1=1+x+x^2+x^4$
C_3	3	$g_3(x)=(x+1)(x^3+x+1)$	$\theta_3=1+x^3+x^5+x^6$
C_4	4	$g_4(x)=x^3+x^2+1$	$\theta_0+\theta_1=x^3+x^5+x^6$
C_5	4	$g_5(x)=x^3+x+1$	$\theta_0+\theta_3=x+x^2+x^4$
C_6	6	$g_6(x)=x+1$	$\theta_0+\theta_3=x+x^2+x^3+x^4+x^5+x^6$

例如，已知$g_2(x)=(x+1)(x^3+x^2+1)$，$h_2(x)=x^3+x+1$时，可以求得幂等生成元为

$$\theta_1(x)=g_2(x)\cdot(x^3+x)=(x^4+x^2+x+1)(x^3+x)$$
$$=x^4+x^2+x+1$$

并且，以$h_2(x)=x^3+x+1$为生成多项式的码C_5的幂等生成元为

$$1+\theta_1(x)=x^4+x^2+x$$

此外，C_2的对偶码以$\tilde{h}_2(x)=x^3+x^2+1$为生成多项式，故$C_4=C_2^{\perp}$的幂等生成元为

$$(1+\theta_1(x))^*=(x^4+x^2+x)^*=x^6+x^5+x^3$$

由于$\tilde{h}_2(x)|g_2(x)$，故由定理4.6.3，C_2是自正交码。同理，C_3也是自正交码。

我们知道，最小循环码C_2只有一个幂等元，即其本原幂等

元 $\theta_1 = 1 + x + x^2 + x^4$。事实上，如果 C_2 有一个非零幂等元，它一定生成 C_2(参看定理 6.4.3 的证明)，而 C_2 有且仅有一个幂等生成元。上述结论对所有的最小循环码都成立。

由定理 4.6.2，$C_1 \subseteq C_4$，$C_2 \subseteq C_4$，可见 $1 + x + x^2 + x^3 + x^4 + x^5 + x^6$，$1 + x + x^2 + x^4$ 和 $x^3 + x^5 + x^6$ 都是 C_4 中的幂等元，其中只有 $x^3 + x^5 + x^6$ 是 C_4 的幂等生成元。

定理 6.4.1 使我们能够直接计算本原幂等元。在我们的例子中，$\theta_1(x)$ 和 $\theta_3(x)$ 的系数分别为

$$\theta_1(x):\ e_i = \alpha^{-i} + \alpha^{-2i} + \alpha^{-4i}$$

$$\theta_3(x):\ e_i = \alpha^{-3i} + \alpha^{-6i} + \alpha^{-5i}$$

由 $\alpha^3 + \alpha + 1 = 0$ 定义的 $GF(2^3)$ 中，容易求出如表 6-1 中所示的 $\theta_1(x)$ 与 $\theta_3(x)$。

因为 $C_2 = \langle\theta_1(x)\rangle$ 的校验多项式为

$$h_2(x) = \prod_{j \in C_1} (x - \alpha^j) = x^3 + x + 1$$

故 C_2 的生成多项式为

$$g_2(x) = (x + 1)(x^3 + x^2 + 1)$$

知道本原幂等元以后，容易求其它码（非最小循环码）的幂等生成元。例如，$C_2 + C_3 (= C_6)$ 的生成多项式为

$$(g_2(x),\ g_3(x)) = x + 1$$

幂等生成元为

$$\theta_1(x) + \theta_3(x) + \theta_1(x)\theta_3(x) = \theta_1(x) + \theta_3(x)$$
$$= x + x^2 + x^3 + x^4 + x^5 + x^6$$

因此，以 C_6 的校验多项式为生成多项式的循环码 C_1 的幂等生成元为

$$1 + \theta_1(x) + \theta_3(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$$

一般地，我们有

定理6.5.1 设 $g(x) = f_1(x)\cdots f_t(x)$，其中 $f_i(x)$ 是 $GF(2)$ 上的既约多项式，且最小循环码 $\langle\hat{g}_i(x)\rangle$ 的本原幂等元为 $\theta_i(x)$，则 $C = \langle g(x)\rangle$ 的幂等元为

$$1+\theta_1(x)+\theta_2(x)+\cdots+\theta_t(x)$$

证明 $\langle \hat{f}_1(x)\rangle+\langle \hat{f}_2(x)\rangle+\cdots+\langle \hat{f}_t(x)\rangle$的校验多项式为$f_1(x)\cdots f_t(x)$，故由推论6.3.4.1，定理6.3.3和定理6.4.2之（1），以$f_1(x)\cdots f_t(x)$为生成多项式的码C的幂等生成元为

$$1+\theta_1(x)+\cdots+\theta_t(x)$$

〈证毕〉

上述定理在实际计算中是很有用的。

例6.5.2 考虑$n=15$时的情形。

在$GF(2)$上有

$$x^{15}+1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

设α为本原多项式x^4+x+1的根，则易得$n=15$时的二元最小循环码（见表6-3)。

表 6-3

码	维数	生成多项式	本原幂等元
μ_0	1	$(x^2+x+1)(x^4+x+1)\cdot(x^4+x^3+1)(x^4+x^3+x^2+x+1)$	$\theta_0=\theta_0^*=1+x+x^2+x^3+\cdots+x^{13}+x^{14}$
μ_1	4	$(x+1)(x^2+x+1)\cdot(x^4+x^3+1)(x^4+x^3+x^2+x+1)$	$\theta_1=\theta_7^*=x+x^2+x^3+x^4+x^6+x^8+x^9+x^{12}$
μ_3	4	$(x+1)(x^2+x+1)\cdot(x^4+x+1)(x^4+x^3+1)$	$\theta_3=\theta_3^*=x+x^2+x^3+x^4+x^6+x^7+x^8+x^9+x^{11}+x^{12}+x^{13}+x^{14}$
μ_5	2	$(x+1)(x^4+x+1)\cdot(x^4+x^3+1)(x^4+x^3+x^2+x+1)$	$\theta_5=\theta_5^*=x+x^2+x^4+x^5+x^7+x^8+x^{10}+x^{11}+x^{13}+x^{14}$
μ_7	4	$(x+1(x^2+x+1)\cdot(x^4+x+1)(x^4+x^3+x^2+x+1)$	$\theta_7=\theta_1^*=x^3+x^6+x^7+x^9+x^{11}+x^{12}+x^{13}+x^{14}$

以此为基础，我们不难求出其它循环码的幂等生成元。例如，C的生成多项式为

$$g(x)=(x^2+x+1)(x^4+x^3+1)$$

则根据定理6.5.1，C的幂等生成元为

$$e(x)=1+\theta_5+\theta_7$$
$$=1+x+x^2+x^3+x^4+x^5+x^6+x^8$$
$$+x^9+x^{10}+x^{12}$$

又如$C=\langle g(x)=(x+1)(x^2+x+1)(x^4+x+1)\rangle$的幂等生成元为

$$e(x)=1+\theta_0+\theta_5+\theta_1$$
$$=x+x^2+x^4+x^8$$

另一方面，因为

$$x+x^2+x^4+x^8=x(x+1)(x^2+x+1)$$
$$(x^4+x+1)$$
$$\triangleq p(x)g(x)$$

而$p(x)$没有引入新的零点，故$\langle p(x)g(x)\rangle=\langle g(x)\rangle$，因此直接验证了$C$的幂等生成元确为$xg(x)$。

§6.6 二次剩余和二次剩余码

为讨论二次剩余码作准备，我们先从二次剩余讲起。

定义6.6.1 设p为奇素数，且$(a, p)=1$。若二次同余方程

$$x^2\equiv a \pmod{p} \tag{6-10}$$

可解，即存在整数x_0，使

$$x_0^2\equiv a \pmod{p}$$

则称a为**模p的二次剩余**。否则，当方程(6-10)无解时，则称a为**模p的二次非剩余**。

例如，取$p=7$，则在模p运算下有

$$1^2\equiv 6^2\equiv 1,\ 2^2\equiv 5^2\equiv 4,\ 3^2\equiv 4^2\equiv 2$$

因此，1、2、4是模7的二次剩余；而3、5、6是模7的二次非剩余。

我们知道，模p的全体剩余类集合$\{\bar{0}, \bar{1}, \cdots, \overline{p-1}\}$构成有限域$GF(p)$。因此，$a$是模$p$的二次剩余系指二次方程

$$x^2=\bar{a}$$

在 $GF(p)$ 中有解，即存在$\bar{x}_0 \in GF(p)$，使

$$\bar{x}_0^2 = \bar{a}$$

于是 a 是模 p 的二次剩余实际上等价于剩余类 $\bar{a}$ 是 $GF(p)$ 的平方元素。此处 $(a, p) = 1$ 的假定，即指 $\bar{a} \neq \bar{0}$。因此当 $\bar{a}$ 是 $GF(p)$ 的平方元素时，二次方程 $x^2 = \bar{a}$ 在 $GF(p)$ 中的解 $\bar{x}_0 \neq \bar{0}$，即 $(p, x_0) = 1$。

当二次方程

$$x^2 = \bar{a}$$

在 $GF(p)$ 内有解时，恰有两个相异解。事实上，若 $\bar{x}_0$ 为其中一个解，则

$$\bar{x}_0^2 = (-\bar{x}_0)^2 = \bar{a}$$

即 $-\bar{x}_0$ 也是方程 $x^2 = \bar{a}$ 的解。但是，$\bar{x}_0 \neq -\bar{x}_0$。否则有 $2\bar{x}_0 = 0$，又因 $GF(p)$ 的特征为 p，故 $p \mid 2$，此与 p 为奇数的假设矛盾。

现在我们进一步研究，在 $GF(p)$ 中有多少个平方元素和非平方元素。

设 α 为 $GF(p)$ 中的本原域元素，则序列

$$\alpha, \ \alpha^2, \ \cdots, \ \alpha^{p-2}, \ \alpha^{p-1} = 1 \tag{6-11}$$

代表 $GF(p)$ 中的全部非零元素。若 α^k 是 $GF(p)$ 中的平方元素，即存在 $\alpha^j \in GF(p)$，使

$$\alpha^k = (\alpha^j)^2 = \alpha^{2j}$$

即 $\alpha^{k-2j} = 1$。因此，$(p-1) \mid (k-2j)$，或

$$k \equiv 2j \pmod{p-1}$$

由于 $p-1$ 为偶数，故 k 必为偶数，即 $k = 2l\left(1 \leqslant l \leqslant \frac{p-1}{2}\right)$。反之若 k 为偶数，则 α^k 显然为平方元素。这表明在 $GF(p)$ 中共有 $\frac{p-1}{2}$ 个平方元素和 $\frac{p-1}{2}$ 个非平方元素。因此，我们得到：

定理6.6.1 设 p 为奇素数，则在与模 p 互素的剩余类集合

$$\bar{1}, \ \bar{2}, \ \cdots, \ \overline{p-1}$$

中，共有 $\frac{p-1}{2}$ 个剩余类是由模 p 的二次剩余构成的，共有

$\frac{p-1}{2}$个剩余类是由模 p 的二次非剩余构成的。

实际上，$\frac{p-1}{2}$ 个剩余类

$$\bar{1}^2,\ \bar{2}^2,\ \cdots,\ \overline{\left(\frac{p-1}{2}\right)}^2 \tag{6-12}$$

显然均由模 p 的二次剩余构成，并且式（6-12）中的剩余类两两不同。否则有

$$\bar{k}^2=\bar{l}^2,\ \bar{k}\neq\bar{l},\ \left(1\leqslant k,\ l\leqslant\frac{p-1}{2}\right)$$

即 $GF(p)$ 上的二次方程 $x^2=\bar{l}^2$ 有 4 个相异解 $\pm\bar{k}$ 及 $\pm\bar{l}$，产生矛盾。

接下来我们讨论整数 a 具备什么条件才是模 p 的二次剩余的问题。

从有限域的角度来看，这一问题等于讨论 $GF(p)$ 中的元素具备什么条件才是平方元素。

由上面的讨论可知，$GF(p)$ 中的任一平方元素都形如 α^{2l} $\left(1\leqslant l\leqslant\frac{p-1}{2}\right)$，从而

$$(\alpha^{2l})^{\frac{p-1}{2}}=(\alpha^{p-1})^l=1$$

反之若任意 $\alpha^k\neq 0\in GF(p)$ 满足条件 $(\alpha^k)^{\frac{p-1}{2}}=1$，即 $\alpha^{\frac{k(p-1)}{2}}=1$，则 $(p-1)\left|\frac{k(p-1)}{2}\right.$，这表明 k 必为偶数。因此 α^k 为平方元素。由此可见，任意 $\beta\neq 0\in GF(p)$ 为平方元素，当且仅当 $\beta^{\frac{p-1}{2}}=1$。另一方面，对任意 $\beta\neq 0\in GF(p)$ 恒有 $\beta^{p-1}=1$。注意到 $p-1$ 为偶数，因此

$$\beta^{p-1}-1=(\beta^{\frac{p-1}{2}}-1)(\beta^{\frac{p-1}{2}}+1)=0$$

上式等式中的两个因子有且仅有一个为零，因为若两个因子同时为零将导致 $2=0$，矛盾。于是，任意 $\beta\neq 0\in GF(p)$ 为非平方元素，当且仅当 $\beta^{\frac{p-1}{2}}=-1$。综上所述，有

定理6.6.2 （欧拉判别准则） 设 p 为奇素数，且 $(a,p)=1$，则

（1） a 为模 p 的二次剩余当且仅当

$$a^{\frac{p-1}{2}}\equiv 1 \pmod{p}$$

（2） a 为模 p 的二次非剩余当且仅当

$$a^{\frac{p-1}{2}}\equiv -1 \pmod{p}$$

推论6.6.2.1

（1） -1 是模 p 的二次剩余当且仅当

$$p\equiv 1 \pmod{4}$$

（2） -1 是模 p 的二次非剩余当且仅当

$$p\equiv -1 \pmod{4}$$

证明 任何奇数必定形如 $4m\pm 1$。若 p 是形如 $4m+1$ 的奇素数，则

$$(-1)^{\frac{p-1}{2}}=(-1)^{\frac{(4m+1)-1}{2}}=(-1)^{2m}=1$$

这表明 -1 是模 p 的二次剩余。若 $p=4m-1$，则

$$(-1)^{\frac{p-1}{2}}=(-1)^{2m-1}=-1\not\equiv 1 \pmod{p}$$

〈证毕〉

推论6.6.2.2

（1） 2 是模 p 的二次剩余当且仅当

$$p\equiv \pm 1 \pmod{8}$$

（2） 2 是模 p 的二次非剩余当且仅当

$$p\equiv \pm 3 \pmod{8}$$

证明 考虑整数序列

$$1,\ 2,\ 3,\ \cdots,\ \frac{p-1}{2} \tag{6-13}$$

及偶数序列

$$2,\ 2\cdot2,\ 2\cdot3,\ \cdots,\ p-1 \tag{6-14}$$

计算式（6-14）中大于$\frac{p-1}{2}$的偶数的个数，亦即求出适合不等式

$$\frac{p-1}{2}<2l\leqslant p-1 \quad 或 \quad \frac{p-1}{4}<l\leqslant\frac{p-1}{2}$$

的整数 l 的个数 ν。显然

$$\nu=\left[\frac{p-1}{2}\right]-\left[\frac{p-1}{4}\right]=\frac{p-1}{2}-\left[\frac{p-1}{4}\right]$$

用 b_1, b_2, $\cdots$, b_ν 代表式（6-14）中大于$\frac{p-1}{2}$的偶数，且 a_1, a_2, $\cdots$, a_λ 代表式（6-14）中小于或等于$\frac{p-1}{2}$的偶数。

令 $\lambda=\frac{p-1}{2}-\nu$。因此

$$\prod_{s=1}^{\lambda}a_s\prod_{t=1}^{\nu}b_t=\prod_{l=1}^{\frac{p-1}{2}}(2l)=\left(\frac{p-1}{2}\right)!\ 2^{\frac{p-1}{2}} \tag{6-15}$$

另一方面，有

$$1=p-(p-1)\leqslant p-b_t<p-\frac{p-1}{2}=\frac{p+1}{2}$$

即 $1\leqslant p-b_t\leqslant\frac{p-1}{2}$。注意到 $p-b_t$ 为奇数，故有

$$a_s\neq p-b_t(s=1,\ \cdots,\ \lambda;\ t=1,\ \cdots,\ \nu)$$

因此 a_s 与 $p-b_t$ 为位于 1 与$\frac{p-1}{2}$之间的$\frac{p-1}{2}$个整数。于是

$$\prod_{s=1}^{\lambda}a_s\prod_{t=1}^{\nu}(p-b_t)=\left(\frac{p-1}{2}\right)! \tag{6-16}$$

但由式（6-15），得

$$\prod_{s=1}^{\lambda} a_s \prod_{t=1}^{\nu} (p-b_t) \equiv \prod_{s=1}^{\lambda} a_s \prod_{t=1}^{\nu} (-b_t)$$

$$\equiv (-1)^{\nu} \prod_{s=1}^{\lambda} a_s \prod_{t=1}^{\nu} b_t$$

$$\equiv (-1)^{\nu} \left(\frac{p-1}{2}\right)! \quad 2^{\frac{p-1}{2}} \pmod{p}$$

故有

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{\nu} \left(\frac{p-1}{2}\right)! \quad 2^{\frac{p-1}{2}} \pmod{p}$$

注意到$\left(p, \left(\frac{p-1}{2}\right)!\right) = 1$，因此

$$2^{\frac{p-1}{2}} \equiv (-1)^{\nu} \pmod{p}$$

任何奇数都形如$8m \pm 1$或$8m \pm 3$。当$p = 8m+1$时，$\nu = \frac{p-1}{2} - \left[\frac{p-1}{4}\right] = 4m - 2m = 2m$；当$p = 8m-1$时，$\nu = (4m-1) - (2m-1) = 2m$。因此当$p = 8m \pm 1$时，

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

即2为模p的二次剩余。当$p = 8m+3$时，$\nu = (4m+1) - 2m = 2m+1$；当$p = 8m-3$时，$\nu = (4m-2) - (2m-1) = 2m-1$。因此当$p = 8m \pm 3$时，

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

由定理6.6.2，推论得证。〈证毕〉

推论6.6.2.3 两个二次剩余的乘积，或两个二次非剩余的乘积都是二次剩余；一个二次剩余和一个二次非剩余的乘积是二次非剩余。

证明 因为

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}}$$

故由定理6.6.2即得本推论。（证毕）

下面，我们定义$GF(2)$上的二次剩余码(习惯上记为QR码)。

设p为奇素数，且$p \equiv \pm 1 \pmod 8$，这意味着2是模p的二次剩余。设α为$GF(2)$的某个扩域上的p次单位原根。令Q表示模p的二次剩余的集合，且令N表示模p的二次非剩余的集合。

由于2是二次剩余，且两个二次剩余之积为二次剩余，故Q为模p的分圆陪集的并集。设2的模p阶为m，则每个分圆陪集含有m个元素。假定共有k个分圆陪集，于是，$km = p-1$。因此Q为$\frac{k}{2}$个分圆陪集的并集，N为其余$\frac{k}{2}$个分圆陪集的并集。

例如，$p=31$时，我们有

$$C_0 = \{0\}$$
$$C_1 = \{1, 2, 4, 8, 16\}$$
$$C_3 = \{3, 6, 12, 24, 17\}$$
$$C_5 = \{5, 10, 20, 9, 18\}$$
$$C_7 = \{7, 14, 28, 25, 19\}$$
$$C_{11} = \{11, 22, 13, 26, 21\}$$
$$C_{15} = \{15, 30, 29, 27, 23\}$$

由于$1^2 \equiv 1$，$3^2 \equiv 9$，$5^2 \equiv 25$，可见

$$Q = C_1 \cup C_5 \cup C_7$$
$$N = C_3 \cup C_{11} \cup C_{15}$$

设

$$q(x) = \prod_{r \in Q}(x - \alpha^r), \quad n(x) = \prod_{n \in N}(x - \alpha^n),$$

则$q(x)$和$n(x)$都是系数取自$GF(2)$上的多项式，并且

$$x^p - 1 = (x-1)\,q(x)\,n(x) \tag{6-17}$$

在§6.6～§6.8中，我们局限于讨论

$$R_p \triangleq GF(2)[x]/(x^p - 1)$$

定义6.6.2 以

$$q(x),\ (x-1)q(x),\ n(x),\ (x-1)n(x)$$

为生成多项式的 R_p 中的循环码都称为 QR 码，并分别记为 Q_1、Q_1'、Q_2 和 Q_2'。

上述定义可以推广到有限域 $GF(l)$ 上，其中 l 是模 p 的二次剩余，即 $l^{\frac{p-1}{2}} \equiv 1 \pmod{p}$。当 $l=2$ 时，这一条件等价于 $p \equiv \pm 1 \pmod{8}$。

由定理4.6.2知，$Q_1' \subseteq Q_1$，$Q_2' \subseteq Q_2$。再由推论4.6.6.1，我们断定 Q_1' 是 Q_1 中那些具有偶数重量的码字所构成的子码。同样 Q_2' 是 Q_2 的偶重量子码。

显然，Q_1 和 Q_2 是 $\left(p,\ \frac{p+1}{2}\right)$ 码，Q_1' 和 Q_2' 是 $\left(p,\ \frac{p-1}{2}\right)$ 码。

为了证明 Q_1 和 Q_2，Q_1' 和 Q_2' 都是等价的 QR 码，我们需要先证明下述定理。这个定理适用于所有的二元循环码。假定码长为 n，其中 n 是奇数。

定理6.6.3 设 α 为 $GF(2)$ 的某个扩域上的 n 次单位原根，K 为 n 的分圆陪集的某个并集。令 $g(x)=\prod_{k\in K}(x-\alpha^k)$，$\breve{g}(x)=\prod_{k\in K}(x-\alpha^{jk})=\prod_{k\in jK}(x-\alpha^k)$，其中 j 是适合 $(j,n)=1$ 的任意整数。令 $c(x)=\sum_{k=0}^{n-1}c_k x^k$ 是 $GF(2)$ 上任意次数 $<n$ 的多项式，且令 $\breve{c}(x)=\sum_{k=0}^{n-1}\breve{c}_k x^k$ 为在置换 $\breve{c}_k=c_m$ ($m \equiv jk \pmod{n}$) 的作用下由 $c(x)$ 得到的多项式。于是，$c(x)\in\langle g(x)\rangle$ 当且仅当 $\breve{c}(x)\in\langle\breve{g}(x)\rangle$。

证明 由于 $(j, n)=1$，故 j 的模 n 逆元素一定存在，设为 i，则 $ij\equiv 1 \pmod{n}$。于是下述论断是彼此等价的：

(1) $c(x)\in\langle g(x)\rangle$

(2) $g(x)|c(x)$

(3) $c(\alpha^k)=0$，对一切 $k\in K$

(4) $c(\alpha^{ik})=0$，对一切 $ik\in K$

(5) $c(\alpha^{ik})=0$，对一切 $k\in jK$

(6) $\check{c}(\alpha^k)=0$，对一切 $k\in jK$

(7) $\check{g}(x)|\check{c}(x)$

(8) $\check{c}(x)\in\langle\check{g}(x)\rangle$

其中（4）和（5）之所以等价，是因为 $ij\equiv 1 \pmod{n}$。(5) 和（6）之所以等价，是因为在置换 $\check{c}_k=c_m$ $(m\equiv jk \pmod{n})$ 的作用下

$$\check{c}(x)=c(x^{j^{-1}})=c(x^i) \tag{6-18}$$

其余的等价关系显然成立。 〈证毕〉

推论6.6.3.1 在置换

$$C_k\rightarrow C_i,\quad i\equiv 2k \pmod{n} \tag{6-19}$$

的作用下，任何二元循环码都是不变的，即上述置换将二元循环码 C 的码字变为 C 的码字。

证明 因为 $2^{-1}K=K$，故

$$\check{g}(x)=\prod_{k\in 2^{-1}K}(x-\alpha^k)=\prod_{k\in K}(x-\alpha^k)=g(x)$$

〈证毕〉

例 6.6.1 再考虑 $n=31$ 时的情形。见表5-4，设 α 为 $GF(2)$ 上5次本原多项式 x^5+x^2+1 的根，并设 $K=C_1\cup C_3$。取 $j=7$，则 $j^{-1}=9$。有

$$g(x)=m^{(1)}(x)m^{(3)}(x)=x^{10}+x^9+x^8+x^6+x^5+x^3+1$$

及

$$\check{g}(x)=m^{(7)}(x)m^{(21)}(x)=x^{10}+x^9+x^4+x^3+1$$

任取 $\langle g(x)\rangle$ 中的一个码字

$$c(x)=(x+1)g(x)$$
$$=x^{11}+x^{8}+x^{7}+x^{5}+x^{4}+x^{3}+x+1$$

则有

$$\check{c}(x)=c(x^{9})=x^{9}+x^{10}+x+x^{14}+x^{5}+x^{27}+x^{8}+1$$
$$=\check{g}(x)(x^{17}+x^{16}+x^{15}+x^{14}+x^{13}$$
$$+x^{12}+x^{7}+x^{5}+x+1)$$

即$\check{c}(x)\in\langle\check{g}(x)\rangle$

如设 $j^{-1}=2$，则 $j=2^{-1}=16$。显然 $16K=K$，并且

$$\check{c}(x)=c(x^{2})=x^{22}+x^{16}+x^{14}+x^{10}+x^{8}+x^{6}+x^{2}+1$$
$$=g(x)(x^{12}+x^{11}+x^{9}+x^{7}+x^{6}+x^{5}+x^{2}+1)$$

因此，$\check{c}(x)\in\langle g(x)\rangle$。从而验证了推论6.6.3.1。

注意如将式（6-19）中的 2 改为 2^{-1}，推论 6.6.3.1 的结论仍然成立，这是因为 $2K=K$ 的原故。

现在我们回过头来讨论 QR 码。

设

$$q(x)=\prod_{r\in Q}(x-\alpha^{r}),\quad n(x)=\prod_{n\in N}(x-\alpha^{n})$$

仍使用定理 6.6.3 中的符号，我们有

$$\check{q}(x)=\prod_{r\in jQ}(x-\alpha^{r}),\quad \check{n}(x)=\prod_{n\in jN}(x-\alpha^{n})$$

根据推论 6.6.2.3，当 $j\in Q$ 时，有

$$jQ=Q,\quad jN=N$$

而当 $j\in N$ 时，有

$$jQ=N,\quad jN=Q$$

因此在定理 6.6.3 中所规定的置换（等价于式（6-18））作用下，我们有

$$\check{q}(x)=q(x),\quad \check{n}(x)=n(x)，\text{对于 } j\in Q$$
$$\check{q}(x)=n(x),\quad \check{n}(x)=q(x)，\text{对于 } j\in N$$

因此由定理6.6.3，得

$$Q_1\to Q_1,\quad Q_2\to Q_2，\text{若 } j\in Q$$

$$Q_1 \to Q_2,\ Q_2 \to Q_1,\ 若\ j \in N$$

对于 Q_1' 和 Q_2'，我们可以得到类似的结果。

此外，由于 $j^{-1} \cdot j \equiv 1 \pmod{p}$，而 1 恒为二次剩余，故 j 和 j^{-1} 同时为模 p 的二次剩余或同时为模 p 的二次非剩余。

综上所述，即得

推论6.6.3.2 对于 QR 码 Q_1，Q_2，Q_1'，Q_2'，在 R_p 中的坐标位置换

$$x \to x^j$$

的作用下，当 $j \in Q$ 时有

$$Q_1 \to Q_1,\ Q_2 \to Q_2,\ Q_1' \to Q_1',\ Q_2' \to Q_2'$$

当 $j \in N$ 时有

$$Q_1 \to Q_2,\ Q_2 \to Q_1,\ Q_1' \to Q_2',\ Q_2' \to Q_1'$$

因此 Q_1 和 Q_2 是相互等价的。同样，Q_1' 和 Q_2' 也相互等价。

定理6.6.4 设 $p \equiv -1 \pmod{8}$，则可以适当选择 α，使得 Q_1，Q_1'，Q_2 和 Q_2' 的幂等生成元分别为

$$\left.\begin{aligned} e_q(x) &= \sum_{r \in Q} x^r,\quad f_q(x) = 1 + \sum_{n \in N} x^n \\ e_n(x) &= \sum_{n \in N} x^n,\quad f_n(x) = 1 + \sum_{r \in Q} x^r \end{aligned}\right\} \tag{6-20}$$

证明 因为 $p \equiv -1 \pmod{8}$，故由推论 6.6.2.1 和推论 6.6.2.2，$2 \in Q$，$-1 \in N$。因为 $e_q^2(x) = \left(\sum_{r \in Q} x^r\right)^2 = \sum_{r \in Q} x^{2r}$ $= \sum_{r \in Q} x^r = e_q(x)$，故 $e_q(x)$ 是幂等元。类似地，式 (6-20) 中的其余 3 个多项式也是幂等元。由引理 6.3.6，$e_q(\alpha^i) = 0$ 或 1。对于任意 $s \in Q$，都有

$$e_q(\alpha^s) = \sum_{r \in Q} \alpha^{rs} = \sum_{r \in Q} \alpha^r = e_q(\alpha)$$

类似地，对于任意 $t \in N$，都有

$$e_q(\alpha^t)=\sum_{r\in Q}\alpha^{rt}=\sum_{r\in Q}\alpha^{-r}=e_q(\alpha^{-1})$$

由引理6.3.2，我们有

$$\begin{aligned}e_q(\alpha)+e_q(\alpha^{-1})&=\sum_{r\in Q}x^r+\sum_{n\in N}x^n\\&=\sum_{i=0}^{p-1}\alpha^i=1\end{aligned}$$

因此根据 α 的选择，我们有

$e_q(\alpha^s)=0$，对一切 $s\in Q$，且 $e_q(\alpha^t)=1$，对一切 $t\in N$ (6-21)

或

$e_q(\alpha^s)=1$，对一切 $s\in Q$，且 $e_q(\alpha^t)=0$，对一切 $t\in N$。

通常我们取 α 使式（6-21）成立。于是，$e_q(x)$ 是 Q_1 的幂等生成元。

因为

$$e_n(\alpha^t)=\sum_{n\in N}\alpha^{nt}=\sum_{r\in Q}\alpha^r=0\text{，对一切 } t\in N$$

及

$$e_n(\alpha^s)=\sum_{n\in N}\alpha^{ns}=\sum_{n\in N}\alpha^n=1\text{，对一切 } s\in Q$$

故 $e_n(x)$ 为 Q_2的幂等生成元。

由于 $f_q(\alpha^s)=0$，对一切 $s\in Q$，且 $f_q(\alpha^t)=1$，对一切 $t\in N$，以及 $f_q(1)=0$，可以断定 $f_q(x)$ 为 Q_1' 的幂等生成元。类似地，$f_n(x)$ 为 Q_2' 的幂等生成元。 〈证毕〉

当 $p\equiv1 \pmod 8$ 时，情况有所不同。这时，Q_1、Q_1'、Q_2 和 Q_2' 的幂等生成元可以分别取为

$$1+\sum_{r\in Q}x^r,\quad \sum_{n\in N}x^n,\quad 1+\sum_{n\in N}x^n,\quad \sum_{r\in Q}x^r$$

请读者自行证明。

例6.6.2 设 α 为 $GF(2^3)$ 上的 7 次单位原根，如果 $GF(2^3)$ 由 $\alpha^3+\alpha+1=0$ 定义，则 Q_1、Q_1'、Q_2 和 Q_2' 的生成多项式分别为

$$(x+\alpha)(x+\alpha^2)(x+\alpha^4)=x^3+x+1$$

$$(x+1)(x^3+x+1)$$

$$(x+\alpha^3)(x+\alpha^6)(x+\alpha^5)=x^3+x^2+1$$

$$(x+1)(x^3+x^2+1)$$

因此 Q_1 和 Q_2 等价于（7，4，3）汉明码；而 Q_1' 和 Q_2' 分别为 Q_1 和 Q_2 的（7，3，4）偶重量子码。此外，Q_1、Q_1'、Q_2 和 Q_2' 的幂等生成元分别为

$$x+x^2+x^4,\quad 1+x^3+x^6+x^5$$

$$x^3+x^6+x^5,\quad 1+x+x^2+x^4$$

例6.6.3 当 $p=23$ 时，我们有

$C_0=\{0\}$

$C_1=\{1,\ 2,\ 4,\ 8,\ 16,\ 9,\ 18,\ 13,\ 3,\ 6,\ 12\}$

$C_5=\{5,\ 10,\ 20,\ 17,\ 11,\ 22,\ 21,\ 19,\ 15,\ 7,\ 14\}$

因为 2 的模 23 阶为 11，故分圆多项式 $Q^{(23)}(x)$ 有两个 11 次的既约因式，设 α 为 23 次单位原根，则 $\frac{1}{\alpha}$ 不属于 α 的共轭元素系，所以 $Q^{(23)}(x)$ 的两个既约因式为互反多项式。利用上述信息，再采用试凑的方法，可以确定

$$x^{23}+1=(x+1)(x^{11}+x^9+x^7+x^6+x^5+x+1)$$

$$(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)$$

设 α 为 11 次本原多项式 $x^{11}+x^9+x^7+x^6+x^5+x+1$ 的根，则 Q_1、Q_1'、Q_2 和 Q_2' 的生成多项式分别为

$$x^{11}+x^9+x^7+x^6+x^5+x+1$$

$$(x+1)(x^{11}+x^9+x^7+x^6+x^5+x+1)$$

$$x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$$

$$(x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)$$

且它们的幂等生成元分别为

$$\sum_{r\in Q} x^r, \quad 1+\sum_{n\in N} x^n, \quad \sum_{n\in N} x^n, \quad 1+\sum_{r\in Q} x^r$$

其中$Q=C_1$，$N=C_5$。

可以证明Q_1和Q_2与（23，12）戈莱码等价。

QR码还有如下重要性质：

定理6.6.5 当$p\equiv-1\pmod 8$时，有

（1）$Q_1=Q_1'+\langle \boldsymbol{h}\rangle$，$Q_2=Q_2'+\langle \boldsymbol{h}\rangle$

$Q_1\cap Q_2=\langle \boldsymbol{h}\rangle$，$Q_1+Q_2=R_p$

（2）$Q_1^{\perp}=Q_1'$，$Q_2^{\perp}=Q_2'$

并且，Q_1'和Q_2'为自正交码。

证明 （1）由定理4.6.5，$Q_1'+\langle \boldsymbol{h}\rangle$的生成多项式为$((x+1)q(x),\ q(x)n(x))=q(x)$，故$Q_1=Q_1'+\langle \boldsymbol{h}\rangle$。同理，$Q_2=Q_2'+\langle \boldsymbol{h}\rangle$。因为$Q_1+Q_2$的生成多项式为$(q(x),\ n(x))=1$，故$Q_1+Q_2=R_p$。根据定理4.6.4，$Q_1\cap Q_2$的生成多项式为$[q(x),\ n(x)]=q(x)n(x)$，因此$Q_1\cap Q_2=\langle \boldsymbol{h}\rangle$。

（2）Q_1的零点为α^r，其中$r\in Q$。由定理4.6.1及互反多项式的性质，我们知道$Q_1^{\perp}$的零点为1和α^{-n}，其中$n\in N$。但因$p\equiv-1\pmod 8$，故由推论6.6.2.1，-1是模p的二次非剩余，从而$-n\in Q$，因此$Q_1^{\perp}$的零点为1和α^r，其中$r\in Q$。这样就证明了$Q_1^{\perp}=Q_1'$。由于$Q_1'\subseteq Q_1$，且$Q_1'^{\perp}=Q_1^{\perp\perp}=Q_1$，故$Q_1'$是自正交码。同理可证，$Q_2^{\perp}=Q_2'$，并且$Q_2'$是自正交码。（证毕）

注意在证明定理中的（1）时，并未用到$p\equiv-1\pmod 8$这一条件，故（1）的结论对于$p\equiv1\pmod 8$也成立。但当$p\equiv1\pmod 8$时，定理之（2）需改为

$$Q_1^{\perp}=Q_2',\quad Q_2^{\perp}=Q_1'$$

请读者自行证明之。

下面我们讨论QR码的生成矩阵。

设Q_1'的幂等生成元为（定理6.6.4）

$$f_q(x)=\sum_{i=0}^{p-1} f_i x^i \tag{6-22}$$

则下述 $p\times p$ 循环矩阵

$$G'=\begin{pmatrix} f_0 & f_1 & \cdots & f_{p-1} \\ f_{p-1} & f_0 & \cdots & f_{p-2} \\ & \cdots & & \cdots \\ f_1 & f_2 & \cdots & f_0 \end{pmatrix} \tag{6-23}$$

是 Q_1' 的一个生成矩阵。显然，G' 的秩为 $\frac{p-1}{2}$。

由上述定理我们知道

$$\begin{pmatrix} & G' & \\ \hline 1 & 1 \cdots & 1 \end{pmatrix} \tag{6-24}$$

是 Q_1 的生成矩阵。对于 Q_2和 Q_2'，我们有类似的结果。

例如当 $p=7$（参看例 6.2.2）时，（7， 4， 3）汉明码Q_1的生成矩阵为

$$\left(\begin{array}{ccccccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

显然这个矩阵的秩为 4 。

§6.7 扩展二次剩余码

我们用通常的增加“全一致校验位”的方法（参看定义 2.6.3）扩展 Q_1 和 Q_2，并记扩展 $Q_1(Q_2)$ 码为 $Q_1(Q_2)$。习惯上我们将新增加的坐标记为∞，因此扩展 QR 码的坐标位可标记为 0， 1，

$\cdots$, $p-1$, ∞。

定理6.7.1 设$p\equiv-1\pmod 8$，则

（1）$\overline{Q}_1$和$\overline{Q}_2$为双偶码；

（2）Q_1和Q_2中的任意码字的重量都与0或3模4同余。

证明 （1）在式（6-24）中增加全一致校验位后，即得$\overline{Q}_1$的一个生成矩阵

$$\overline{G}=\begin{pmatrix} & G' & & \begin{matrix}0\\0\\\vdots\\0\end{matrix} \\ 1 & 1 & \cdots\ 1 & 1\end{pmatrix} \tag{6-25}$$

（列标：$0\quad 1\quad \cdots\quad p-1\quad \infty$）

由于$p=-1+8k$，故模p的二次剩余和二次非剩余各有$\frac{p-1}{2}=4k-1$个。因此$\overline{G}$的行重量皆为4的倍数。因为Q_1'是自正交码（定理6.6.5），故G'中的行彼此正交，并显然与h正交。因此由定理2.7.2，$\overline{Q}_1$为双偶码。类似地可以证明：$\overline{Q}_2$也是双偶码。这里我们作一个注记：显然$\overline{Q}_1$和$\overline{Q}_2$是$\left(p+1,\frac{p+1}{2}\right)$码，其中$p+1=8k$，这正是双偶码存在的充分必要条件。

（2）由（1）的结果，$\overline{Q}_1$和$\overline{Q}_2$中任意码字的重量皆为4的倍数；而Q_1和Q_2分别为$\overline{Q}_1$和$\overline{Q}_2$的删除码，因此Q_1和Q_2中任意码字的重量$\equiv 0$或$3\pmod 4$。 〈证毕〉

注意类似于定理6.7.1，当$p\equiv1\pmod 8$时，有如下结果：

（1）$\overline{Q}_1^{\perp}=\overline{Q}_2$，$\overline{Q}_2^{\perp}=\overline{Q}_1$

（2）$\overline{Q}_1$和$\overline{Q}_2$只含有偶重量向量。

在证明本节的主要定理（6.7.7）之前，我们需要引入一些

新的概念。

回忆我们讲过的置换群。设 π_1，…，π_k 为 k 个 n 次置换，我们称 π_1，…，π_k **生成一个群** G，并记为 $G=\langle\pi_1, \cdots, \pi_k\rangle$，如果 G 是包含 π_1，…，π_k 的 S_n 中的最小子群。显然子群 G 必须包含生成置换 π_1，…，π_k 的所有形式的方幂的乘积。

我们称集合 $S=\{a_1, \cdots, a_n\}$ 上的置换群 G 为**传递群**，如果对于任意的 a_i，$a_j\in S$，都存在一个置换 $\pi\in G$，使得 $\pi(a_i)=a_j$。更一般地，称 G 为 **t—重传递群**，如果给定 t 个彼此不同的 a_{i_1}，…，$a_{i_t}\in S$ 和 t 个不同的 a_{j_1}，…，$a_{j_t}\in S$，都存在一个置换 $\pi\in G$，使得 $\pi(a_{i_1})=a_{j_1}$，…，$\pi(a_{i_t})=a_{j_t}$。

例如，令 $S=\{1, 2, \cdots, 7\}$，且 $\pi=(1, 2, 3, 4, 5, 6, 7)$ 为循环移位置换，则 $G=\langle\pi\rangle$ 是由 π 的方幂组成的 7 阶循环群。更进一步，G 是 S 上的传递群，因为给定 i，$j\in S$，总存在某个 k，使得 $\pi^k(i)=j$。

又如，$S_3=\langle(1, 2), (1, 2, 3)\rangle$ 或 $S_3=\langle(2, 3), (1, 3, 2)\rangle$…(参看例 3.5.3)，等等。

我们感兴趣的是对码的坐标位置所进行的置换。设 $\boldsymbol{a}=(a_1, \cdots, a_n)$ 是一个向量，而 π 是一个 n 次置换，则 $\pi(\boldsymbol{a})=(\pi(a_1), \cdots, \pi(a_n))$。例如，$\pi$ 是 7 次循环移位置换，即 $\pi=(1, 2, 3, 4, 5, 6, 7)$，而 $\boldsymbol{a}=(1\ 0\ 0\ 1\ 0\ 1\ 1)$，则 $\pi(\boldsymbol{a})=(1\ 1\ 0\ 0\ 1\ 0\ 1)$。

这样一来，我们可以用另外一种方式定义循环码。设 π 为 n 次循环移位置换，C 为二元 (n, k) 码，则 C 为循环码，当且仅当若 $c\in C$，则 $\pi(c)\in C$。因此，在循环移位置换 π（或 π^i）的作用下，循环码 C 的生成矩阵变为 C 的另一个生成矩阵。

显然，对二元 (n, k) 码 C 的坐标位所进行的任意 n 次置换都将 C 变为一个等价的 (n, k) 码或 C 本身。容易证明，所有将 C 变成它自己的置换构成一个群，因而我们有下述定义。

定义6.7.1 所有将 C 变为它自己的坐标位置的置换，构成 **C 的自同构群**，记为 $G(C)$。

由定义可知，$G(C)$ 是 S_n 的一个子群。此外，由 $G(C)$ 和 $G(C^{\perp})$ 的定义立即可得

定理6.7.2 $G(C)=G(C^{\perp})$。

例6.7.1

（1）设 C 为整个空间，则显然有

$$G(C)=S_n。$$

（2）回忆重复码 $C_R=\langle h\rangle$。因为

$$C_R=\{0\ 0\cdots 0,\ \ 1\ 1\cdots 1\}$$

显然有 $G(C_R)=S_n$。

（3）由定理6.7.2，对于偶重量码 $C_E=C_R^{\perp}$，也有 $G(C_E)=S_n$。

例如，当 $n=3$，$k=2$ 时，C_E 的生成矩阵和一致校验矩阵分别为

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},\ (1\quad 1\quad 1),$$

可见，$C_E=\{0\ 0\ 0,\ 0\ 1\ 1,\ 1\ 0\ 1,\ 1\ 1\ 0\}$。读者容易直接验证该偶重量码的自同构群为

$$S_3=\{(1),(1,2),(1,3),(2,3),(1,2,3),(1,3,2)\}$$

（4）设（4，2）码 C 的生成矩阵为

$$G=\begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 \end{matrix} \\ \hline \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

则 $G(C)$ 的阶为8，且

$$G(C)=\{(1),(1,2),(3,4),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(1,3,2,4),(1,4,2,3)\}$$

一般而言，确定码的自同构群是很困难的。求码的自同构群的生成置换，甚至有时由生成置换求 $G(C)$ 的阶，也是很困难

的。通常求$G(C)$的一个子群则比较容易。

显然我们可以用$n \times n$矩阵A来表示坐标位的置换。例如，3次置换$\pi=(2,\ 3)$可以用3×3矩阵A如下表示

$$\begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ A=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

定理6.7.3 设$(n,\ k)$码的生成矩阵为G，则用$n\times n$矩阵A表示的坐标位置的置换属于$G(C)$当且仅当

$$KG=GA$$

其中K是某个$k\times k$可逆矩阵。

证明 $A\in G(C)$当且仅当GA是C的一个生成矩阵，当且仅当通过初等变换能由G获得GA。 〈证毕〉

注意在上面的证明过程中，我们用到了矩阵代数中的下述性质：若A为域F上的$n\times n$可逆矩阵，则A为有限个初等矩阵的乘积。

例6.7.2 我们定义二元单形码C_r为二元$(n=2^r-1,\ n-r)$汉明码的对偶码。因此，C_r是$(2^r-1,\ r)$码，且其生成矩阵G_r为它所对应的汉明码的一致校验矩阵。

例如

$$G_2=\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

因此

$$C_2=\{0\,0\,0,\ 0\,1\,1,\ 1\,0\,1,\ 1\,1\,0\}$$

又如

$$\begin{array}{c} \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ G_3=\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

是 C_3 的一个生成矩阵。

用归纳法可以证明，C_r 的所有非零码字的重量都等于 2^{r-1}。这就是单形码名称的由来。

命

$$A=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

则 7×7 矩阵 A 代表 7 次置换

$$\pi=(0)(1,\ 4,\ 2)(3,\ 5,\ 6)$$

它将 C_3 变为 C_3 自己。事实上，我们有

$$G_3A=\begin{array}{c} \begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

$$=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}G_3=KG_3$$

其中 K 为 3×3 可逆矩阵。

定义6.7.2　域 F 上所有 $k\times k$ 可逆矩阵的集合称为**一般线性群**，并记为 $GL(k,\ F)$。若 F 为有限域 $GF(q)$，则记为 $GL(k,\ q)$。

定理6.7.4　一般线性群 $GL(k,\ q)$ 的阶为

$$(q^k-1)(q^k-q)(q^k-q^2)\cdots(q^k-q^{k-1})$$

证明　设 $K\in GL(k,\ q)$。于是 K 中的第 1 列可为 $GF(q)$ 中的任意非零向量，故共有 q^k-1 种选取方法。K 的第 2 列不能

为第 1 列的倍数，因此共有 q^k-q 种选取方法。类似地，K的第 3 列不能为前两列的线性组合，故共有 q^k-q^2种选取方法。如此继续下去，可见 $GF(q)$ 上秩为 k 的 $k\times k$ 矩阵共有

$$(q^k-1)(q^k-q)(q^k-q^2)\cdots(q^k-q^{k-1})$$

个。由矩阵代数可知，$k\times k$ 矩阵K为可逆矩阵当且仅当 rank $K=k$。 〈证毕〉

由定理 6.7.3 可知，二元（n，k）码C的自同构群$G(C)$与 $GL(k,\ 2)$ 的一个子群同构。

定理6.7.5 设（n，k）码C中所有码字的重量都是偶数，且有如下性质：无论删除哪个坐标，所得的删除码的重量分布都相同。命$\{A_i\}$表示C的重量分布，且$\{a_i\}$表示删除码的重量分布，则有

$$a_{2j-1}=\frac{2jA_{2j}}{n}$$

$$a_{2j}=\frac{n-2j}{n}A_{2j}$$

此外，删除码的最小距离为奇数。

证明 考虑C中由重量为 $2j$ 的 A_{2j}个码字所组成的矩阵M，显然M中共有 $2jA_{2j}$ 个 1。由定理的假设，M中各列含有 1 的数目相同，且等于 a_{2j-1}。因此

$$a_{2j-1}=\frac{2jA_{2j}}{n}$$

由于 $A_{2j}=a_{2j}+a_{2j-1}$，故有

$$a_{2j}=A_{2j}-a_{2j-1}=\frac{n-2j}{n}A_{2j}$$

显然删除码的最小距离为奇数。 〈证毕〉

现在我们来讨论扩展 QR 码的自同构群。

定义6.7.3 设 p 为素数，且 $p\equiv\pm1\pmod 8$，则坐标位置$\{0,\ 1,\ 2,\ \cdots,\ p-1,\ \infty\}$上的所有如下形状

$$y\to\frac{ay+b}{cy+d} \tag{6-26}$$

的置换构成一个群，称为**特殊射影线性群**，并记为 $PSL_2(p)$，其中 a，b，c，$d\in GF(p)$，且满足条件

$$ad-bc=1$$

$PSL_2(p)$ 的主要性质是

定理6.7.6

（1）$PSL_2(p)$ 由下述 3 个置换生成：

$$S:\ y\to y+1$$

$$V:\ y\to \rho^2 y \qquad (6\text{-}27)$$

$$T:\ y\to -\frac{1}{y}$$

其中 ρ 为 $GF(p)$ 中的本原域元素。

（2）$PSL_2(p)$ 的阶为 $\frac{1}{2}p(p^2-1)$。$PSL_2(p)$ 由下述 $\frac{1}{2}p(p^2-1)$ 个置换组成：

$$V^iS^j:\ y\to \rho^{2i}y+j \qquad (6\text{-}28)$$

$$V^iS^jTS^k:\ y\to k-(\rho^{2i}y+j)^{-1} \qquad (6\text{-}29)$$

其中 $0\leqslant i<\frac{1}{2}(p-1)$，$0\leqslant j$，$k<p$。

（3）$PSL_2(p)$ 为传递群。

证明 当 $c=0$ 时，有 $d=\frac{1}{a}$，故

$$\frac{ay+b}{cy+d}=a^2y+ab$$

当 $c\neq 0$ 时，有 $b=\frac{ad-1}{c}$，因此

$$\frac{ay+b}{cy+d}=\frac{ay+\frac{ad-1}{c}}{cy+d}=\frac{acy+ad-1}{c(cy+d)}$$

$$=\frac{a}{c}-\frac{1}{c^2y+cd}$$

综合上面的讨论，设

$$y \to \frac{ay+b}{cy+d}, \quad ad-bc=1$$

是 $PSL_2(p)$ 中的任意元素，则可将它改写为

$$y \to a^2y+ab, \quad \text{对于 } c=0 \tag{6-30}$$

或

$$y \to \frac{a}{c}-\frac{1}{c^2y+cd}, \quad \text{对于 } c \neq 0 \tag{6-31}$$

经过简单的计算即可验证，式（6-28）相当于 V^iS^{ab}，其中 $a=\rho^i$；式（6-29）相当于 $V^iS^{cd}TS^{a/c}$，其中 $c=\rho^i$。

在式（6-30）中，令 $ab=j$，即得式（6-28）；在式(6-31)中，令 $\frac{a}{c}=k$，$cd=j$，即得式(6-29)；其中 $0 \leqslant i < \frac{1}{2}(p-1)$，$0 \leqslant j$，$k < p$。

式（6-28）中共有 $\frac{1}{2}(p-1)p$ 个置换，式（6-29）中共有 $\frac{1}{2}(p-1)p^2$ 个置换，因此 $PSL_2(p)$ 的阶为

$$\frac{1}{2}(p-1)p+\frac{1}{2}(p-1)p^2$$

$$=\frac{1}{2}p(p-1)(p+1)$$

最后，因为通过 S 的方幂可以将任意有限坐标变为任意其它的有限坐标，而 T 可以交换 0 与∞，因此对于任意坐标位置 i 和 j，都存在 $PSL_2(p)$ 中的一个置换，能将 i 变为 j，即 $PSL_2(p)$ 为传递群。 〈证毕〉

在这里我们作一个注记。式（6-27）中的生成置换 V 是多余的，亦即 S 和 T 就可以生成 $PSL_2(p)$。

下述定理是十分重要的。

定理6.7.7 扩展 QR 码的自同构群包含 $PSL_2(p)$。换言之，在 $PSL_2(p)$ 的作用下，$\overline{Q}_1$ 和 $\overline{Q}_2$ 都固定不变。

证明 由于 S 是循环移位置换，而 V 不改变幂等元，故在 S 和 V 的作用下，$Q_i(i=1, 2)$ 固定不变，即 $S, V \in G(Q_i)$。

又因为 S 和 V 都将 ∞ 变为 ∞，故 S，$V\in G(\overline{Q}_l)$。剩下来只需证明，T 也使 $\overline{Q}_l$ 固定不变。

为简单计，我们只考虑 $p=7$ 的情形。这时，扩展（8，4，4）汉明码 $\overline{Q}_1$，有形如式（6-25）的生成矩阵 $\overline{G}$：

$$\begin{array}{c} \\ r_0 \\ r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \\ r_6 \\ r_\infty \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty \end{array} \\ \left(\begin{array}{ccccccc|c} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right) \end{array} \qquad (6\text{-}32)$$

并将上述矩阵中的各行分别记为 $\boldsymbol{r}_0$，$\boldsymbol{r}_1$，…，$\boldsymbol{r}_6$ 和 $\boldsymbol{r}_\infty$。

在 T 的作用下，$\overline{G}$ 变为 $\overline{G}'$。在我们的例子中

$$T=(0,\ \infty)(1,\ 6)(2,\ 3)(4,\ 5)$$

因此，可以由 $\overline{G}$ 通过交换 0 和 ∞ 列、1 和 6 列、2 和 3 列、4 和 5 列得到 $\overline{G}'$，如式（6-33）所示。

$$\overline{G}'=\begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty \end{array} \\ \left(\begin{array}{cccccccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right) \end{array} \begin{array}{l} \\ =r_0+h \\ =r_6+r_0+h \\ =r_3+r_0+h \\ =r_2+r_0 \\ =r_5+r_0+h \\ =r_4+r_0 \\ =r_1+r_0 \\ =r_\infty \end{array} \qquad (6\text{-}33)$$

由此可见，$T(\boldsymbol{r}_0)=\boldsymbol{r}_0+\boldsymbol{h}$，$T(\boldsymbol{r}_1)=\boldsymbol{r}_6+\boldsymbol{r}_0+\boldsymbol{h}$，…，$T(\boldsymbol{r}_\infty)=\boldsymbol{r}_\infty$。因此，在 T 的作用下，$\overline{G}$ 中的任意行都变为 $\overline{Q}_1$ 中的一个码字。显然，$\overline{G}'$ 也是 $\overline{Q}_l$ 的一个生成矩阵。

当 $p\equiv-1\pmod 8$ 时，可以证明下述一般情形：

$$T(\boldsymbol{r}_0)=\boldsymbol{r}_0+\boldsymbol{h}$$

$$T(\boldsymbol{r}_s)=\boldsymbol{r}_{-s^{-1}}+\boldsymbol{r}_0+\boldsymbol{h}，\text{对于 } s\in Q$$

$$T(r_i) = r_{-i^{-1}} + r_0,\ 对于\ i \in N$$
$$T(r^{\infty}) = r_{\infty}$$

〈证毕〉

定理6.7.8

（1）扩展 QR 码的所有删除码都等价。

（2）QR 码 Q_1 和 Q_2 的最小重量为奇数。

证明

（1）由定理 6.7.6，我们知道，$PSL_2(p)$ 是扩展 QR码的坐标{0，1，…，$p-1$，∞}上的传递群，即对于任意坐标位置 i 和 j，都存在一个 $PSL_2(p)$ 中的置换，能将 i 变为 j，并使扩展 QR 码保持不变。因此删除扩展 QR 码的第 i 列和第 j 列后所得到的删除码等价。

（2）由于扩展 QR 码满足定理 6.7.5 中的条件，因此QR码 Q_1和 Q_2(作为扩展 QR 码的删除码）的最小重量为奇数。

〈证毕〉

§6.8 二次剩余码的纠错能力和译码

对于 QR 码（只考虑 Q_1 和 Q_2）纠错能力的研究，下述定理是最重要的。

定理6.8.1 （平方根限）

（1）设 d 为 QR 码 Q_1或 Q_2 的最小重量，则

$$d^2 \geqslant p \tag{6-34}$$

（2）更进一步，当 $p \equiv -1 \pmod 8$ 时，有

$$d^2 - d + 1 \geqslant p \tag{6-35}$$

证明

（1）设 $a(x)$ 为 Q_1 中具有最小重量 d 的码字。设 $n \in N$，则由推论 6.6.3.2 可知，$b(x) = a(x^n)$ 是 Q_2 中具有最小重量 d 的码字（注意 Q_1 和 Q_2等价）。所以

$$a(x)b(x) \in Q_1 \cap Q_2 = \langle h \rangle$$

根据定理 6.7.8，d 为奇数，故 $a(x)b(x) \neq 0$（读者可自行

证明)。因此 $a(x)b(x)=h$。从而 $a(x)b(x)$ 的重量为 p。但是，乘积 $a(x)b(x)$ 中具有非零系数的项不能超过 d^2 个（$a(x)$ 和 $b(x)$ 的重量皆为 d），于是 $d^2 \geqslant p$。

（2）当 $p \equiv -1 \pmod 8$ 时，由推论 6.6.2.1 可知，-1 为模 p 的二次非剩余，故（1）中的 n 可取为 -1。设

$$a(x)=a_0+a_1x+\cdots+a_mx^m$$

则

$$a(x^{-1})=a_0+a_1x^{-1}+\cdots+a_mx^{-m}$$

显而易见，乘积 $a(x)a(x^{-1})$ 中有 d 项等于 1。因为 d 为奇数，故上述 d 项之和为 1。因此 $a(x)a(x^{-1})$ 中最多含有 $d^2-(d-1)$ 个非零项，即 $d^2-d+1 \geqslant p$。〈证毕〉

由定理 6.7.8 中的（2）和定理 6.7.1 中的（2）可知，当 $p \equiv -1 \pmod 8$ 时，Q_1 和 Q_2 的最小重量都 $\equiv 3 \pmod 4$。利用这一事实，可以根据平方根限（定理 6.8.1）计算 $p \leqslant 72$ 时的扩展 QR 码的最小重量表（见表 6-4）。

例如，当 $p=23$ 时，由于 $3^2-3+1=7<23$，故 $d \geqslant 7$。因此扩展（24，12）QR 码的最小重量 $d \geqslant 8$。但是上述（24，12）码中有一个重量为 8 的码字，故 $d=8$。类似地，当 $p=47$ 时，由于 $7^2-7+1=43<47$，故 $d \geqslant 11$。因此扩展（48，24）QR 码的最小重量 $d=12$。

平方根限只给出 d 的下限。但表 6-4 给出了某些二元扩展 QR 码的最小重量。这是因为在这些码中都找到了一个重量等于

表 6-4

$p \equiv -1 \pmod 8$				$p \equiv 1 \pmod 8$			
p	n	k	d	p	n	k	d
7	8	4	4	17	18	9	6
23	24	12	8	41	42	21	8
31	32	16	8				
47	48	24	12				
71	72	36	12				

平方根限所限定的值的码字。

虽然对表 6-4 中的码，平方根限给出了真实的最小距离。但是随着 p 值的增大，平方根限也越来越弱。

以下对二元 QR 码和扩展 QR 码进行了小结。

二元QR码和扩展QR码小结

Q_1，Q_1'，Q_2 和 Q_2' 的生成多项式分别为

$$g(x)=\prod_{r\in Q}(x+\alpha^r),\ (x+1)g(x),$$

$$n(x)=\prod_{n\in N}(x+\alpha^n),\ (x+1)n(x)$$

其中 α 为 $GF(2)$ 的某个扩域上的 p 次单位原根。

QR 码具有如下性质：

码长 p = 素数，且 $p\equiv\pm1\ (\mathrm{mod}\ 8)$，

$$\dim Q_1=\dim Q_2=\frac{1}{2}(p+1),$$

$$\dim Q_1'=\dim Q_2'=\frac{1}{2}(p-1),$$

$$Q_1=Q_1'+\langle \boldsymbol{h}\rangle,\ Q_2=Q_2'+\langle \boldsymbol{h}\rangle,$$

$$Q_1\cap Q_2=\langle \boldsymbol{h}\rangle,\ Q_1+Q_2=R_p,$$

Q_1 与 Q_2 等价，Q_1' 与 Q_2' 等价，

最小距离 $d\geqslant\sqrt{p}$ 且 d 为奇数（对 Q_1 和 Q_2）。

当 $p\equiv-1\ (\mathrm{mod}\ 8)$ 时，

Q_1，Q_1'，Q_2 和 Q_2' 的幂等生成元可分别取为

$$\sum_{r\in Q}x^r,\quad 1+\sum_{n\in N}x^n,\quad \sum_{n\in N}x^n,\quad 1+\sum_{r\in Q}x^r$$

当 $p\equiv 1\ (\mathrm{mod}\ 8)$ 时，

Q_1，Q_1'，Q_2 和 Q_1' 的幂等生成元可分别取为

$$1+\sum_{r\in Q}x^r,\quad \sum_{n\in N}x^n,\quad 1+\sum_{n\in N}x^n,\quad \sum_{r\in Q}x^r$$

当 $p\equiv-1\ (\mathrm{mod}\ 8)$ 时，还有

$$Q_1^{\perp}=Q_1',\ \ Q_2^{\perp}=Q_2',$$

Q_1' 和 Q_2' 为自正交码，

Q_1 或 Q_2 的最小重量 $d\equiv 3\pmod 4$，

且满足关系 $d^2-d+1\geqslant p$，

当 $p\equiv 1\pmod 8$ 时，还有

$$Q_1^{\perp}=Q_2',\ \ Q_2^{\perp}=Q_1'。$$

扩展 QR 码 $\overline{Q}_1$ 和 $\overline{Q}_2$ 在 $PSL_2(p)$ 的作用下固定不变。此外当 $p\equiv -1\pmod 8$ 时，我们有

$\overline{Q}_1$ 和 $\overline{Q}_2$ 为双偶码。

当 $p\equiv 1\pmod 8$ 时，我们有

$$\overline{Q}_1^{\perp}=\overline{Q}_2,\ \ \overline{Q}_2^{\perp}=\overline{Q}_1$$

$\overline{Q}_1$ 和 $\overline{Q}_2$ 中仅含偶重量码字。

对 QR 码的总评价是，QR 码是一类译码比较困难的"好"码。称它为"好"码，是因为我们已知许多中等大小的 QR 码的最小重量 d，相对于码长 p 而言，d 是相当大的。我们自然会问，当码长 p 增加时，d 的变化情况将如何？然而，对任何码类解答这一问题都是非常困难的。一般而言，对于"好"的、且具有一定结构的 $(n,k(n),d(n))$ 码类，我们总是希望当 n 增加时，$\frac{d(n)}{n}$ 和 $\frac{k(n)}{n}$ 都有一个不等于零的下界。对于 QR 码，它的信息率 $\frac{k(p)}{p}$ 约为 $\frac{1}{2}$，显然其下界不为零。至于 QR 码的译码，可以采用下述所谓"**置换译码**"的方法。

设 C 为二元 (n,k,d) 码。假定 $\boldsymbol{v}=(v_0,v_1,\cdots,v_{n-1})$ 为传送的码字（即发送向量），且错误向量 $\boldsymbol{e}=(e_0,e_1,\cdots,e_{n-1})$ 的重量 $\leqslant t$，其中 $2t+1\leqslant d$。于是接收向量 $\boldsymbol{r}=\boldsymbol{v}+\boldsymbol{e}=(r_0,r_1,\cdots,r_{n-1})$。为简单起见，我们假定 C 是系统码（参看定理 2.2.2），即 C 的生成矩阵为 $G=[A\,|\,I]$，一致校验矩阵为 $H=[I\,|\,A^T]$，用 A^T 表示 A 的转置矩阵。因此 $(v_0,\cdots,v_{n-1})$ 是码

字中的$m=n-k$个校验位，而$(v_m, \cdots, v_{n-1})$则构成C的信息组。

定理6.8.2 设错误向量$\boldsymbol{e}=(e_0, e_1, \cdots, e_{n-1})$的重量$\leqslant t$，其中$d\geqslant 2t+1$。设接收向量$\boldsymbol{r}=(r_0, r_1, \cdots, r_{n-1})$的伴随式为$\mathbf{s}^T=H\boldsymbol{r}^T$。若$w(\mathbf{s}^T)\leqslant t$，则信息组$(r_m, \cdots, r_{n-1})$是正确无误的，且$\boldsymbol{s}^T=(e_0, e_1, \cdots, e_{m-1})^T$给出了错误格式。若$w(\mathbf{s}^T)>t$，则信息组中至少有一位出错。

证明 （1）设信息组是正确的，即对于$m\leqslant i\leqslant n-1$，都有$e_i=0$。于是$s^T=H\boldsymbol{r}^T=[I\mid A^T]\boldsymbol{r}^T=[I\mid A^T]\boldsymbol{e}^T=(e_0, e_1, \cdots, e_{m-1})^T$，并且$w(\mathbf{s}^T)\leqslant t$。

（2）命$\boldsymbol{e}_{(1)}=(e_0, e_1, \cdots, e_{m-1})$，$\boldsymbol{e}_{(2)}=(e_m, \cdots, e_{n-1})$，并假设$\boldsymbol{e}_{(2)}\neq 0$。考虑$v=\boldsymbol{e}_{(2)}G=\boldsymbol{e}_{(2)}[A\mid I]=(\boldsymbol{e}_{(2)}A\mid\boldsymbol{e}_{(2)})\neq 0$，因为$v$是$C$中的一个非零码字，故由定理的假定，$w(v)\geqslant 2t+1$。因此$w(\boldsymbol{e}_{(2)})+w(\boldsymbol{e}_{(2)}A)\geqslant 2t+1$。由于

$$\mathbf{s}^T=H\boldsymbol{e}^T=[I\mid A^T]\begin{pmatrix}\boldsymbol{e}^T_{(1)}\\ \boldsymbol{e}^T_{(2)}\end{pmatrix}=\boldsymbol{e}^T_{(1)}+A^T\boldsymbol{e}^T_{(2)}$$

故有

$$\begin{aligned}w(\mathbf{s}^T)&\geqslant w(A^T\boldsymbol{e}^T_{(2)})-w(\boldsymbol{e}^T_{(1)})\\&=w(\boldsymbol{e}_{(2)}A)-w(\boldsymbol{e}_{(1)})\\&=(w(\boldsymbol{e}_{(2)}A)+w(\boldsymbol{e}_2))-(w(\boldsymbol{e}_{(1)})\\&\quad+w(\boldsymbol{e}_{(2)}))\\&\geqslant 2t+1-w(\boldsymbol{e})\\&\geqslant t+1\end{aligned}$$

〈证毕〉

注意在上述定理的证明中用到了下述结论：设$\boldsymbol{a}$与$\boldsymbol{b}$为$GF(2)$上的两个向量，则有

$$w(\boldsymbol{a}+\boldsymbol{b})\geqslant w(\boldsymbol{a})-w(\boldsymbol{b})$$

请读者自行证明。

上述定理是置换译码方法的基础。置换译码是一种借助于码

的自同构群的译码方案，可用于一般的循环码。码的自同构群越大，这一方法就越有效。

对于某个固定的 t，其中 $t\leqslant\left[\frac{d-1}{2}\right]$，假定要纠正所有重量$\leqslant t$的错误向量，置换译码的基本思想是，利用$G(C)$中的置换找到接收向量 $\boldsymbol{r}$ 中不出错的信息组。下面我们举例予以说明。

例6.8.1 设C为（7，4，3）QR码Q_1，则它有下述的生成矩阵和一致校验矩阵：

$$G=\begin{array}{c}\begin{array}{ccccccc}0&1&2&3&4&5&6\end{array}\\ \left(\begin{array}{ccccccc}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\1&1&1&0&0&1&0\\1&0&1&0&0&0&1\end{array}\right)\end{array}=[A|I] \qquad (6-36)$$

$$H=\begin{array}{c}\begin{array}{ccccccc}0&1&2&3&4&5&6\end{array}\\ \left(\begin{array}{ccccccc}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{array}\right)\end{array}=[I|A^T] \qquad (6-37)$$

设发送的码字为$\boldsymbol{v}=(0，1，0，0，0，1，1)$，错误向量$\boldsymbol{e}=(0，0，0，1，0，0，0)$，即信息组的坐标位置3出了一个错。因此接收向量为$\boldsymbol{r}=(0，1，0，1，0，1，1)$。

计算接收向量$\boldsymbol{r}$的伴随式

$$\boldsymbol{s}^T=H\boldsymbol{r}^T=H\boldsymbol{e}^T=(1，1，0)^T$$

正如定理6.8.2所预期的那样

$$w(\boldsymbol{s}^T)=2>t\ (=1)$$

由此可见，$\boldsymbol{r}$的信息组中至少有一位出错。

我们求具有下述性质的$G(C)$中的一组置换$P=\{\pi_1=1，\pi_2，\cdots，\pi_j\}$，对于任意重量$\leqslant t$的错误向量$\boldsymbol{e}$，都存在某个$\pi_i\in$

P，使e中的1分量都分布在除信息组以外的坐标位上。

在例子中，可以取$P=\{1, S^2, S^4\}$，其中S是定理6.7.6中定义的循环移位置换。若$e=(0, 0, 0, 1, 0, 0, 0)$，则$S^4(e)=(1, 0, 0, 0, 0, 0, 0)$，因此，$S^4$使$e$的信息组中不再含有1分量。

一般而言，对每一种码都要计算一次P。但是求最小置换集合P是一件容易的事情。如果P不是最小的集合，仍然可以使用，只不过效率比较差而已。

置换集合$P=\{1, S^2, S^4\}$的作用见表6-6。

表 6-6

	信息组
$v=(v_0, v_1, v_2,$	$v_3, v_4, v_5, v_6)$
$S^2(v)=(v_5, v_6, v_0,$	$v_1, v_2, v_3, v_4)$
$S^4(v)=(v_3, v_4, v_5$	$v_6, v_0, v_1, v_2)$

注意，P的选取方法并非只有一种。例如，在表6-6中，取$P=\{1, S^3, S^6\}$也可以达到同样目的。请读者予以验证。

计算$S^4(r)$的伴随式，有

$$s^T=H(1, 0, 1, 1, 0, 1, 0)^T=(1, 0, 0)^T$$

因此由$w(s^T)=1$可知，信息组$\{0, 1, 2, 6\}$中没有发生错误，且错误格式$s^T=(1, 0, 0)^T$说明第3个坐标位出错。

由上面的讨论，我们将$S^4(r)$与$(1, 0, 0, 0, 0, 0, 0)$相加，得$w=(0, 0, 1, 1, 0, 1, 0)$。最后将r译为$S^3(w)=(0, 1, 0, 0, 0, 1, 1)$(注意，$S^3$是$S^4$的逆变换)，恢复了原发送码字。

我们总结置换译码的方法如下：

(1) 根据前面所述的要求，选取$G(C)$中的最小置换集合

$$P=\{\pi_1=1, \pi_2, \cdots, \pi_j\}$$

(2) 设r为接收向量，依次计算$\pi_i(r)$和它的伴随式

$$S^{(i)T}=H(\pi_i(r))^T$$

直到找到一个 i，使得

$$w(S^{(i)T}) \leqslant t$$

这样一来，根据定理6.8.2，我们知道所有的错误都分布在 $\pi_i(r)$ 中的前 m 位，并由 $(e_0, e_1, \cdots, e_{m-1}) = S^{(i)}$ 给定。因此令

$$w = \pi_i(r) + (e_0, e_1, \cdots, e_{m-1}, 0, \cdots, 0)$$

并将 r 译为 $\pi_i^{-1}(w)$。

（3）如果对所有的 i，恒有

$$w(S^{(i)T}) > t$$

则译码器判定 r 中出现了 $\geqslant t+1$ 个错误。

下面我们介绍一种置换译码方法的变形。我们用同一个例子予以说明。

由式（6-37）可得 C 的一致校验方程

$$\left.\begin{aligned} a_0 &= a_3 + a_5 + a_6 \\ a_1 &= a_3 + a_4 + a_5 \\ a_2 &= a_4 + a_5 + a_6 \end{aligned}\right\} \qquad (6\text{-}38)$$

仍设发送码字为 $v=(0, 1, 0, 0, 0, 1, 1)$，接收向量为 $r=(0, 1, 0, 1, 0, 1, 1)$。根据 r 的信息组（因为信息组的坐标位置集合为 $I=\{3, 4, 5, 6\}$），利用式(6-38)进行编码，就得到 C 中一个码字

$$w_1 = (1, 0, 0, 1, 0, 1, 1)$$

计算 w_1 和 r 之间的距离，有

$$d(w_1, r) = 2 > t$$

这说明 r 的信息组中至少有一位发生了错误。仍取 $G(C)$ 中的最小置换集合

$$P = \{1, S^2, S^4\}$$

在 S^2 的作用下，式（6-38）变为

$$\left.\begin{aligned} a_2 &= a_0 + a_1 + a_5 \\ a_3 &= a_0 + a_5 + a_6 \\ a_4 &= a_0 + a_1 + a_6 \end{aligned}\right\} \qquad (6\text{-}39)$$

注意这时的信息组为 $S^2(I) = \{0, 1, 5, 6\}$

类似地，根据新的信息组{0，1，5，6}，利用式(6-39)计算 w_2，得

$$w_2=(0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 1)$$

这一次，有

$$d(w_2,\ r)=1=t$$

因此我们将 r 译为 w_2，从而恢复了原发送码字。

(7，4，3)QR 码的置换译码过程见表6-7。

表 6-7

0	1	2	3	4	5	6	
0	1	0	0	0	1	1	v：发送码字
0	1	0	1	0	1	1	r：接收向量
1	0	0	1	0	1	1	w_1：利用 $I=\{3,\ 4,\ 5,\ 6\}$ 计算的向量
0	1	0	0	0	1	1	w_2：利用 $S^2(I)=\{0,\ 1,\ 5,\ 6\}$ 计算的向量

我们将上述方法小结如下：

(1) 选取 $G(C)$ 中的置换集合

$$P=\{\pi_1=1,\ \pi_2,\ \cdots,\ \pi_j\}$$

(2) 设 I 为信息组，E_1 为 C 的一致校验方程。利用 I 和 E_1 计算出向量 w_1；

(3) 若 $d(w_1,\ r)\leqslant t$，则将 r 译为 w_1。否则，计算在 π_2 的作用下，由 E_1 得到的新的一致校验方程 E_2；

(4) 利用 $\pi_2(I)$ 和 E_2 计算出向量 w_2；

(5) 若 $d(w_2,\ r)\leqslant t$，则将 r 译为 w_2。否则，重复上述过程，直到求出一个 i，$1\leqslant i\leqslant j$，使得 $d(w_i,\ r)\leqslant t$。于是我们将 r 译为 w_i；

(6) 如果对任意 i，$1\leqslant i\leqslant j$，恒有

$$d(w_i,\ r)>t,$$

则译码器判断 r 中出现的错误多于 t 个。

显然上述两种置换译码的方法实质上是相同的，它们都源于定理6.8.2。

§6.9 BCH 码

在介绍一般的 t—纠错 BCH 码以前，我们简要地对 §5.11 中讲过的二元双纠错 BCH 码作一小结。为此先证明一个引理。

设 α 为 $GF(2^m)$ 上的 n 次单位原根，仍记 $m^{(i)}(x)$ 为 α^i 的最小多项式。我们有

引理6.9.1 设 $m\geqslant 3$，且 $n=2^m-1$，则有

（1）$m^{(1)}(x)\neq m^{(3)}(x)$

（2）$\deg m^{(1)}(x)=\deg m^{(3)}(x)=m$

证明 考虑 $n=2^m-1$ 的分圆陪集 C_1 和 C_3。显然有

$$C_1=\{1,\ 2,\ 2^2,\ \cdots,\ 2^{m-2},\ 2^{m-1}\}$$

$$|C_1|=m$$

并且

$$C_3=\{3,\ 3\cdot 2,\ 3\cdot 2^2,\cdots,3\cdot 2^{m-2},\ 2^{m-1}+1\}\qquad(6\text{-}40)$$

式（6-40）之所以成立，是因为

（a）$3\cdot 2^{m-2}=2^m-2^{m-2}<2^m-1\ (m\geqslant 3)$

（b）$3\cdot 2^{m-1}=2^m+2^{m-1}>2^m-1$

因此

$$3\cdot 2^{m-1}-(2^m-1)=2^{m-1}+1$$

（c）$2\cdot(2^{m-1}+1)=2^m+2>2^m-1$

所以

$$2\cdot(2^{m-1}+1)-(2^m-1)=3$$

由此可见，$C_1\neq C_3$，并且$|C_3|=|C_1|=m$。（证毕）

定理6.9.1 二元双纠错 BCH 码 C 是以

$$g(x)=m^{(1)}(x)m^{(3)}(x)$$

为生成多项式的循环码，并具有参数

$(n=2^m-1,\ k=n-2m,\ d\geqslant 5)$，$m\geqslant 3$。

证明 在 §5.11 中，我们定义码长为 $n=2^m-1$ 的双纠错

BCH 码的一致校验矩阵

$$H=\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^m-2)} \end{pmatrix} \tag{6-41}$$

我们有

$c\in C$，当且仅当 $Hc'=O$

当且仅当 $\sum_{i=0}^{n-1} c_i\alpha^i=0$ 且 $\sum_{i=0}^{n-1} c_i\alpha^{3i}=0$

当且仅当 $c(\alpha)=0$ 且 $c(\alpha^3)=0$

当且仅当 $m^{(1)}(x)|c(x)$ 且 $m^{(3)}(x)|c(x)$

当且仅当 $[m^{(1)}(x),m^{(3)}(x)]|c(x)$。

因为 $m^{(1)}(x)$ 和 $m^{(3)}(x)$ 都是既约多项式，且由引理6.9.1可知，$m^{(1)}(x)\neq m^{(3)}(x)$，故有

$$[m^{(1)}(x),m^{(3)}(x)]=m^{(1)}(x)m^{(3)}(x)$$

因此

$c\in C$ 当且仅当 $m^{(1)}(x)m^{(3)}(x)|c(x)$，

即 C 是以 $g(x)=m^{(1)}(x)m^{(3)}(x)$ 为生成多项式的循环码。

再由引理6.9.1，得 $\deg g(x)=2m$，故

$$\dim C=n-2m$$

至于 $d\geqslant 5$，已在§5.11中给予证明（参看定理6.9.2的又一种证明方法）。 （证毕）

下面我们讨论一般情形。

设 V_n 表示 $GF(q)$ 上的 n 维向量空间，且设 $(n,q)=1$。我们知道，V_n 与剩余类代数 $GF(q)[x]\mathrm{mod}(x^n-1)$ 或与 $GF(q)$ 上 $\langle x\rangle$ 的群代数 FG 同构。

设 m 为 q 的模 n 阶，即 m 是满足 $q^m\equiv 1(\mathrm{mod}\ n)$ 的最小正整数，又设 α 为 $GF(q^m)$ 中的 n 次单位原根。

定义6.9.1 称 $GF(q)$ 上码长为 n 的循环码为**设计距离是 δ 的BCH码**，如果其生成多项式

$$g(x)=[m^{(b)}(x),m^{(b+1)}(x),\cdots,m^{(b+\delta-2)}(x)] \tag{6-42}$$

其中 b、δ 均为整数，且 $b\geqslant 0$，$\delta\geqslant 1$。亦即 $g(x)$ 以 α 的 $\delta-1$ 个接续的方幂

$$\alpha^b,\ \alpha^{b+1},\ \cdots,\ \alpha^{b+\delta-2}$$

为零点。因此，$\boldsymbol{c}$ 是一个码字当且仅当

$$c(\alpha^b)=c(\alpha^{b+1})=\cdots=c(\alpha^{b+\delta-2})=0 \qquad (6\text{-}43)$$

特别，当 $b=1$ 时，我们称相应的 BCH 码为**狭义BCH码**。当 $n=q^m-1$ 时，我们称它们为**本原BCH 码**，而当 $n<q^m-1$ 时，我们称它们为**非本原BCH码**。

由定义可见，当 b 固定时，BCH 码是嵌套的，亦即设计距离为 δ_1 的码包含设计距离为 δ_2 的码，当且仅当 $\delta_1\leqslant\delta_2$。

一般地讲，BCH 码的对偶码不再是 BCH 码。

对于一般的循环码，求它的最小距离是非常困难的。BCH 码的一个主要特点，就在于 BCH 码求出了码的最小距离与其生成多项式的根之间的联系，从而给出了估计码的最小距离的下限，使我们可以设计具有事先给定纠错能力的循环码。

定理6.9.2 （BCH 限）设计距离为 δ 的 BCH 码 C 的最小距离 $d\geqslant\delta$。

证明 由式（6-43）可知，BCH 码 C 的一致校验矩阵可写为

$$H=\begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ 1 & \alpha^{b+2} & \alpha^{2(b+2)} & \cdots & \alpha^{(n-1)(b+2)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{pmatrix} \qquad (6\text{-}44)$$

现在证明 H 矩阵的任何 $\delta-1$ 列都线性独立。为此我们研究由 H 矩阵的任何 $\delta-1$ 列所构成的行列式

$$D=\begin{vmatrix} \alpha^{a_1 b} & \cdots & \alpha^{a_{\delta-1} b} \\ \alpha^{a_1(b+1)} & \cdots & \alpha^{a_{\delta-1}(b+1)} \\ \vdots & \cdots & \vdots \\ \alpha^{a_1(b+\delta-2)} & \cdots & \alpha^{a_{\delta-1}(b+\delta-2)} \end{vmatrix}.$$

提出每一列的公因子，即得

$$D=\alpha^{t(a_1+\cdots+a_{\delta-1})}\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{a_1} & \alpha^{a_2} & \cdots & \alpha^{a_{\delta-1}} \\ \alpha^{2a_1} & \alpha^{2a_2} & \cdots & \alpha^{2a_{\delta-1}} \\ \vdots & & \cdots & \vdots \\ \alpha^{(\delta-2)a_1} & \alpha^{(\delta-2)a_2} & \cdots & \alpha^{(\delta-2)a_{\delta-1}} \end{vmatrix} \tag{6-45}$$

上式右端的行列式是范德蒙德（Vander-monde）行列式

$$V(x_1,\ x_2,\ \cdots,\ x_n)=\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$$

为计算$V(x_1,\ x_2,\ \cdots,\ x_n)$，考虑函数

$$V(x_1,\ \cdots,\ x_{n-1},\ x)=\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ x_1 & x_2 & \cdots & x_{n-1} & x \\ x_1^2 & x_2^2 & \cdots & x_{n-1}^2 & x^2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_{n-1}^{n-1} & x^{n-1} \end{vmatrix} \tag{6-46}$$

我们将$V(x_1,\ x_2,\ \cdots,\ x_{n-1},\ x)$视为$x$的多项式，显然它以$x_1,\ x_2,\ \cdots,\ x_{n-1}$为根。例如，当$x=x_1$时，上面的行列式中第一列与最后一列相同，从而行列式之值为零。因此

$$V(x_1,\ x_2,\ \cdots,\ x_{n-1},\ x)=A(x-x_1)(x-x_2)\cdots(x-x_{n-1}) \tag{6-47}$$

显然A即为$V(x_1,\ x_2,\ \cdots,\ x_{n-1},\ x)$中$x^{n-1}$的系数。所以

$$A=V(x_1,\ x_2,\ \cdots,\ x_{n-1})$$

这表明

$$V(x_1,\ x_2,\ \cdots,\ x_{n-1},\ x)=V(x_1,\ x_2,\ \cdots,\ x_{n-1})(x-x_1)\cdots(x-x_{n-1}) \tag{6-48}$$

在式（6-48）中令$x=x_n$，即得下述递推公式：

$$V(x_1, x_2, \cdots, x_{n-1}, x_n)=V(x_1, x_2, \cdots, x_{n-1})(x_n-x_1)\cdots(x_n-x_{n-1}) \tag{6-49}$$

因为$V(x_1, x_2)=x_2-x_1$，故有

$$V(x_1, x_2, x_3)=V(x_1, x_2)(x_3-x_1)(x_3-x_2)$$
$$=(x_2-x_1)(x_3-x_1)(x_3-x_2)$$

反复应用式（6-49），最后得

$$V(x_1, x_2, \cdots, x_n)=\prod_{i>j}^{n}(x_i-x_j) \tag{6-50}$$

把这一结果应用到式（6-45）中，有

$$D=\alpha^{b(a_1+\cdots+a_{\delta-1})}\prod_{i>j}^{\delta-1}(\alpha^{a_i}-\alpha^{a_j})$$

注意到α为n次单位原根，且

$$0\leqslant a_j<a_i\leqslant n-1$$

故上式乘积中任何因式皆不为零，于是$D\neq 0$。这表明H矩阵中任何$\delta-1$列均线性独立。根据定理2.5.4，BCH码C的最小距离$d\geqslant\delta$ 〈证毕〉

作为这一定理的直接应用，我们考虑二元双纠错BCH码。它的生成多项式$g(x)=m^{(1)}(x)m^{(3)}(x)$。因为$m^{(1)}(\alpha)=m^{(1)}(\alpha^2)=m^{(1)}(\alpha^4)=0$，且$m^{(3)}(\alpha^3)=0$，故该BCH码有4个接续零点：$\alpha$，$\alpha^2$，$\alpha^3$，$\alpha^4$，因此$d\geqslant 5$，与§5.11中的讨论相符合。

注意，在设计距离为δ的BCH码的H矩阵（6-44）中，如果将每个阵元都用相应的$GF(q)$上的m重代替，就得到一个$m(\delta-1)$行的矩阵。但是这些行不一定全部线性独立，因此该BCH码的维数$k\geqslant n-m(\delta-1)$。综上所述，得

定理6.9.3 设C为$GF(q)$上码长为n且设计距离为δ的BCH码，则有

$$\dim C\geqslant n-m(\delta-1)$$

其中m为q的模n阶。

今后我们主要讨论狭义BCH码。如果从$b=0$而不是从

$b=1$ 出发，就将得到狭义 BCH 码的偶重量子码。

下面我们讨论二元 BCH 码。

在二元情形，最小多项式有如下性质：

$$m^{(i)}(x)=m^{(2i)}(x)$$

因此我们总可以假定二元狭义 BCH 码的设计距离 δ 为奇数。这时，设计距离为 $\delta=2t$ 和设计距离为 $\delta=2t+1$ 的 BCH 码是相同的，它们都以

$$g(x)=[m^{(1)}(x),\ m^{(3)}(x),\ \cdots,\ m^{(2t-1)}(x)]$$

为生成多项式。

但是，$\deg m^{(i)}(x)\leqslant m\ (i=1,\ 3,\ \cdots,\ 2t-1)$，故 $\deg g(x)\leqslant mt$，因此 BCH 码的维数 $\geqslant n-mt$。

此外，BCH 码的一致校验矩阵

$$H=\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ & \cdots & & \cdots & \\ 1 & \alpha^{2t-1} & \cdots & \cdots & \alpha^{(2t-1)(n-1)} \end{pmatrix}$$

其中每个阵元都表示某个二元 m 重。H 矩阵中的第 2 列只需要包含下述 α 之方幂：α^1，α^{a_1}，α^{a_2}，$\cdots$，其中 1，a_1，a_2，$\cdots$ 属于不同的分圆陪集。

综上所述，我们有

定理6.9.4 对于任何正整数 m 和 $t\leqslant 2^{m-1}-1$，都存在一个码长为 $n=2^m-1$ 的二元 t—纠错 BCH 码 C，并且

$$\dim C\geqslant n-mt$$

这一定理充分显示出 BCH 码的优越性。的确，由于以上原因，再加上 BCH 码的有效的译码方法，使 BCH 码在实践中得到广泛应用。

例6.9.1 求所有码长为 $n=2^4-1=15$ 和 $n=2^5-1=31$ 的二元狭义本原 BCH 码。

利用 § 5.9 中所求出的 $GF(2^4)$ 和 $GF(2^5)$ 上元素的最小多项式表，我们很容易得到码长 $n=15$ 的二元 BCH 码（见表6-8）

和码长 $n=31$的二元 BCH 码（见表6-9）。

表 6-8

设计距离 δ	生成多项式 $g(x)$	$g(x)$的根的方幂（α的方幂）	维 数 $k=n-\deg g(x)$	真实最小距离 d
1	1	—	15	1
3	$m^{(1)}(x)$	1, 2, 4, 8	11	3
5	$m^{(1)}(x)m^{(8)}(x)$	1—4, 6, 8, 9, 12	7	5
7	$m^{(1)}(x)m^{(3)}(x)$ $m^{(5)}(x)$	1—6, 8—10, 12	5	7
9, 11, 13 或 15	$m^{(1)}m^{(3)}m^{(5)}m^{(7)}$ $=\frac{x^{15}+1}{x+1}$	1—14	1	15

表 6-9

设计距离 δ	生成多项式 $g(x)$	维 数 $k=n-\deg g(x)$	真实最小距离 d
1	1	31	1
3	$m^{(1)}$	26	3
5	$m^{(1)}m^{(3)}$	21	5
7	$m^{(1)}m^{(3)}m^{(5)}$	16	7
9 或11	$m^{(1)}m^{(3)}m^{(5)}m^{(7)}$	11	11
13或15	$m^{(1)}m^{(3)}m^{(5)}m^{(7)}m^{(11)}$	6	15
17, 19, …, 31	$m^{(1)}m^{(3)}m^{(5)}m^{(7)}m^{(11)}m^{(15)}$	1	31

由表6-8和表6-9我们看到，具有不同设计距离的 BCH 码有可能重合。例如，由表 5-7 可知，$m^{(9)}(x)=m^{(5)}(x)$。因此设计距离 $\delta=9$ 和 $\delta=11$ 的两个码长 $n=31$ 的二元 BCH 码是相同的，它们都以

$$g(x)=m^{(1)}(x)m^{(3)}(x)m^{(5)}(x)m^{(7)}(x)$$

为生成多项式。

如果BCH码C_1，…，C_l重合，且它们的设计距离分别为δ_1，…，δ_l，则称

$$\delta = \max_{1 \leqslant i \leqslant l} \delta_i$$

为上述BCH码的**波斯**（**Bose**）**距离**。由BCH限可知，BCH码的真实最小距离不小于它的波斯距离。

在表6-8、表6-9中，恰好有$d=\delta$（波斯距离）。下面的例子告诉我们，BCH限并不是紧致的，即有可能$d>\delta$。

例6.9.2 根据例6.6.3的结果，我们有

$$x^{23}+1=(x+1)m^{(1)}(x)m^{(5)}(x)$$

其中

$$m^{(1)}(x)=x^{11}+x^9+x^7+x^6+x^5+x+1$$
$$m^{(5)}(x)=x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$$

由于

$$m^{(1)}(x)=m^{(3)}(x)$$

可见设计距离为$\delta=3$和$\delta=5$的两个码长为$n=23$的二元狭义BCH码重合，它们的生成多项式皆为

$$g(x)=m^{(1)}(x)$$

它们的一致校验矩阵为

$$H=(1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{22})$$

其中每个阵元都对应一个2元11重。该码的维数$k=23-\deg g(x)=12$。

码长$n=23$的二元BCH码见表6-10。

表 6-10

设计距离 δ	生成多项式 $g(x)$	α的方幂	维数 $k=n-\deg g(x)$	真实最小距离 d
1	1	—	23	1
3或5	$m^{(1)}(x)$	1—4，6，8，9，12，13，16，18	12	7
7，9，…，23	$m^{(1)}(x)m^{(5)}(x)$	1—22	1	23

我们可以证明，上述码长 $n=23$ 的二元狭义非本原 BCH 码 $\langle m^{(1)}(x)\rangle$ 与 $(23,12,7)$ 戈莱码等价，因此它的真实最小距离（$d=7$）大于它的波斯距离（$\delta=5$）。

一般而言，求 BCH 码的真实最小距离 d 是很困难的。然而在特定的情况下，我们有可能解决这一问题。

定理6.9.5 （彼得森（Peterson））设 $n=ab$，则码长为 n 且设计距离为 a 的二元 BCH 码 C 的最小距离 $d=a$。

证明 设 α 为 n 次单位原根，则

$$\alpha^{ib}\neq 1,\ \text{对一切}\ i<a \tag{6-51}$$

由于

$$x^n-1=(x^b)^a-1=(x^b-1)(1+x^b+x^{2b}+\cdots+x^{(a-1)b})$$

故 α，α^2，…，α^{a-1} 不是 x^b-1 的零点，否则与式（6-51）相矛盾。因此上述 $a-1$ 个接续的 α 的方幂都是

$$1+x^b+x^{2b}+\cdots+x^{(a-1)b} \tag{6-52}$$

的零点。于是式（6-52）是 C 中一个重量为 a 的码字。所以 $d=a$。 〈证毕〉

例如，在码长为 $n=15$ 的二元 BCH 码中，当 $\delta=3$ 或 5 时，$d=3$ 或 5，如表6-8所示。

又如，对于 $n=63$ 的二元 BCH 码，当 $\delta=3$，7，9，21 时，分别有 $d=3$，7，9，21。

上述定理对非本原二元 BCH 码也成立。

因此对于码长 $n=21$ 的非本原二元 BCH 码，当 $\delta=3$ 或 7 时，分别有 $d=3$ 或 7。

最后我们阐述 BCH 码译码的梗概。

尽管BCH 码的译码问题已经能够通过逻辑电路加以实现，但这不等于说它的译码手续已经充分简单。我们只扼要地介绍一下 BCH 码的译码思想。至于详细的译码过程，读者可参看书末所列的有关参考文献。

为简单起见，我们不妨设 $b=1$，$\delta=2t+1$，于是相应的（狭义）BCH 码 C 至少可以纠正 t 个错误。假设

$$\mathbf{c}=(c_0,\ c_1,\ \cdots,\ c_{n-1})=c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$$

为码向量，而

$$\mathbf{r}=(r_0,\ r_1,\ \cdots,\ r_{n-1})=\mathbf{r}(x)=r_0+r_1x+\cdots+r_{n-1}x^{n-1}$$

为接收向量，同时

$$\mathbf{e}=(E_0,\ E_1,\ \cdots,\ E_{n-1})=e(x)=E_0+E_1x+\cdots+E_{n-1}x^{n-1}$$

为错误向量。于是

$$r(x)=c(x)+e(x)$$

且C的一致校验矩阵由

$$H=\begin{pmatrix}1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1}\\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)}\\ & & \cdots\cdots & & \\ 1 & \alpha^{2t} & \alpha^{4t} & \cdots & \alpha^{2t(n-1)}\end{pmatrix}$$

给出。

译码的第一步，就是根据H矩阵计算伴随式

$$\mathbf{s}=[s_1,\ s_2,\ \cdots,\ s_{2t}]=[r_0,\ r_1,\ \cdots,\ r_{n-1}]H'$$

其中s_k由下式决定：

$$s_k=r(\alpha^k)=c(\alpha^k)+e(\alpha^k)=e(\alpha^k)=\sum_{i=0}^{n-1}E_i\alpha^{ik}$$

$$k=1,\ 2,\ \cdots,\ 2t$$

设有e个错误出现（$1\leqslant e\leqslant t$），则对应于这e个错误的E_i不为零。不妨把V_n中向量的第1位分量（$0\leqslant i\leqslant n-1$）叫作第$\alpha^i$位的分量。如果$e$的从左往右数的第$j$个（$1\leqslant j\leqslant e$）非零分量是$E_i$，则称$X_j=\alpha^i$为这个错误$E_i$的**错位**，而称$Y_j=E_i$为这个错误的**错值**。显然$X_j\in GF(q^m)$，而$Y_j\in GF(q)$。于是我们可以将$s_k$写成

$$s_k=\sum_{j=1}^{e}Y_jX_j^k \tag{6-53}$$

置

$$\sigma(z)=\prod_{i=1}^{e}(1-X_i z) \tag{6-54}$$

显然$\sigma(z)$以各个错位的倒数X_1^{-1}，X_2^{-1}，…，X_e^{-1}为其全部根。如能求出$\sigma(z)$的全部根，便可立即定出错误X_1，X_2，…，X_e。因此，称$\sigma(z)$为**错误定位多项式**。经验告诉我们，处理根为错位倒数（即$GF(q^m)$中的乘法逆元素）的多项式比处理根的错误位置本身的多项式更为方便。

由于$s_k=r(\alpha^k)$对一切$k\geqslant 1$均能定义，因此我们可以引进形式幂级数（或称作序列$\{s_k\}$的生成函数）

$$s(z)=\sum_{k=1}^{\infty}s_k z^k \tag{6-55}$$

根据式（6-53），我们有

$$s(z)=\sum_{k=1}^{\infty}s_k z^k=\sum_{k=1}^{\infty}z^k\sum_{j=1}^{e}Y_j X_j^k$$

$$=\sum_{j=1}^{e}Y_j\sum_{k=1}^{\infty}(X_j z)^k=\sum_{j=1}^{e}\frac{Y_j X_j z}{1-X_j z}$$

令

$$\omega(z)=s(z)\sigma(z) \tag{6-56}$$

则

$$\omega(z)=\sum_{j=1}^{e}\frac{Y_j X_j z}{1-X_j z}\prod_{i=1}^{e}(1-X_i z)$$

$$=\sum_{j=1}^{e}Y_j X_j z\prod_{i\neq j}(1-X_i z) \tag{6-57}$$

显然$\omega(z)$是次数$\leqslant e$的多项式。

命

$$\sigma(z)=\sum_{i=0}^{e}\sigma_i z^i$$

由式（6-56）与式（6-57），比较等式两边 z 的同次幂的系数，再注意到式（6-56）中 z^{e+1}，z^{e+2}，…的系数为零，即得

$$\left.\begin{aligned}\sigma_0 s_{e+1}+\sigma_1 s_e+\cdots+\sigma_e s_1&=0\\ \sigma_0 s_{e+2}+\sigma_1 s_{e+1}+\cdots+\sigma_e s_2&=0\\ \vdots\qquad\quad \vdots\qquad\qquad\quad \vdots\quad&\\ \sigma_0 s_{2t}+\sigma_1 s_{2t-1}+\cdots+\sigma_e s_{2t-e}&=0\end{aligned}\right\}\tag{6-58}$$

我们可以将式（6-58）视为一个包含未知量 σ_0，σ_1，…，σ_e 和已知量 s_1，s_2，…，s_{2t} 的方程组。原则上，如果从方程组（6-58）能够解得 σ_0，σ_1，…，σ_e，就可以求出 $\sigma(z)$ 和 $\omega(z)$，从而可以求得错位 X_j；再在 $\omega(z)$ 中置 $z=X_j^{-1}$，即可求出错值 Y_j。但是实际上我们解这个方程组时会遇到一个严重的问题，亦即译码器事先并不知道 e 的值。下面的定理从理论上解决了这个问题。

定理6.9.6 假定 $\hat{e}$ 是适合下述条件的最小整数：存在一个次数 $\leqslant\hat{e}$ 的多项式 $\hat{\sigma}(z)$，满足 $\hat{\sigma}(0)=1$，并且在乘积 $\hat{\sigma}(z)s(z)$ 中，$z^{\hat{e}+1}$，$z^{\hat{e}+2}$，…，z^{2t} 的系数均为零。于是，$\hat{e}=e$，$\hat{\sigma}(z)=\sigma(z)$。

证明 由于 $\sigma(z)$ 适合条件 $\sigma(0)=1$，且在乘积 $\sigma(z)s(z)$ 中，z^{e+1}，z^{e+2}，…，z^{2t} 的系数均为零。因此 $\hat{e}\leqslant e$。

置

$$\hat{\sigma}(z)=\sum_{l=0}^{\hat{e}}\hat{\sigma}_l z^l$$

并在乘积 $\hat{\sigma}(z)s(z)$ 中，令 $z^{\hat{e}+1}$，$z^{\hat{e}+2}$，…，z^{2t} 的系数均为零，则得

$$\begin{aligned}\sum_{l=0}^{\hat{e}}\hat{\sigma}_l s_{k-l}&=\sum_{l=0}^{\hat{e}}\hat{\sigma}_l\sum_{j=1}^{e}Y_j X_j^{k-l}\\ &=\sum_{j=1}^{e}Y_j X_j^{k}\sum_{l=0}^{\hat{e}}\hat{\sigma}_l X_j^{-l}\end{aligned}$$

$$= \sum_{j=1}^{e} \hat{\sigma}(X_j^{-1}) Y_j X_j^k = 0 \text{。}$$

$$(k = \hat{e}+1,\ \hat{e}+2,\ \cdots,\ 2t)$$

将上式看作是以 $\hat{\sigma}(X_j^{-1})Y_j$ （$j=1,\ 2,\ \cdots,\ e$）为未知量，以X_j^k($j=1,\ 2,\ \cdots,\ e$；$k=\hat{e}+1,\ \hat{e}+2,\ \cdots,\ 2t$)为已知量的$2t-\hat{e}$个方程的线性方程组，这一方程组的系数矩阵为

$$\begin{pmatrix} X_1^{\hat{e}+1} & X_2^{\hat{e}+1} & \cdots & X_e^{\hat{e}+1} \\ X_1^{\hat{e}+2} & X_2^{\hat{e}+2} & \cdots & X_e^{\hat{e}+2} \\ \vdots & \vdots & \cdots & \vdots \\ X_1^{2t} & X_2^{2t} & \cdots & X_e^{2t} \end{pmatrix}$$

它具有 $2t-\hat{e}$ 行和 e 列。注意我们有

$$2t-\hat{e} \geqslant 2t-e \geqslant e$$

而该矩阵的前 e 行及前 e 列构成范德蒙德行列式.它显然不为零，因此上面这个矩阵的秩为e。由线性方程组的理论可知，上述的方程组只有零解：

$$\hat{\sigma}(X_1^{-1})Y_1 = 0,\ \hat{\sigma}(X_2^{-1})Y_2 = 0,\ \cdots,\ \hat{\sigma}(X_e^{-1})Y_e = 0 \text{。}$$

由于Y_1，Y_2，$\cdots$，Y_e均不为零，故

$$\hat{\sigma}(X_1^{-1}) = 0,\ \hat{\sigma}(X_2^{-1}) = 0,\ \cdots,\ \hat{\sigma}(X_e^{-1}) = 0 \text{。}$$

这表明 $\hat{\sigma}(z)$也以X_1^{-1}，X_2^{-1}，$\cdots$，X_e^{-1} 为根。因此

$$\hat{\sigma}(z) = \sigma(z),\ \hat{e} = e$$

〈证毕〉

这一定理把求$\sigma(z)$ 的问题归结为求 $\hat{\sigma}(z)$。从译码的角度来看，这是关键的一步。伯勒凯布（Berle kamp）给出了求$\hat{\sigma}(z)$ 的一种迭代算法，从而使 BCH 码的译码比较容易实现。关于这一算法的修正，则由梅西（Massey）给出。

例6.9.3 设α为由$\alpha^4+\alpha+1=0$定义的$GF(2^4)$ 中的本原域元素。假定我们采用的是码长为$n=15$、设计距离为$\delta=5$的狭义 BCH 码，且接收向量为

$$r(x) = 1 + x^2 + x^4 + x^7 + x^8 + x^{11} + x^{12} + x^{13} + x^{14}$$

试用刚才讲过的方法译出这个向量。

解　在我们的情形，$t=2$。先利用关系式

$$s_k = r(\alpha^k)$$

计算出 s_1，s_2，s_3 和 s_4。借助于表5-1，可以求得

$$s_1=\alpha, \quad s_2=\alpha^2, \quad s^3=0, \quad s_4=\alpha^4$$

方程组（6-58）形如

$$\left.\begin{aligned} \sigma_0 s_3+\sigma_1 s_2+\sigma_2 s_1=0 \\ \sigma_0 s_4+\sigma_1 s_3+\sigma_2 s_2=0 \end{aligned}\right\}$$

将上述结果代入，则得

$$\left.\begin{aligned} \alpha^2\sigma_1+\alpha\sigma_2=0 \\ \alpha^4+\alpha^2\sigma_2=0 \end{aligned}\right\}$$

解得

$$\sigma_1=\alpha, \quad \sigma_2=\alpha^2$$

亦即

$$\sigma(z)=1+\alpha z+\alpha^2 z^2 \tag{6-59}$$

将式（6-59）写成

$$\sigma(z)=(1-X_1 z)(1-X_2 z)$$

的形状，有

$$\sigma(z)=(1-\alpha^6 z)(1-\alpha^{11} z)$$

因此错位是

$$X_1=\alpha^6, \quad X_2=\alpha^{11}$$

于是我们将 $r(x)$ 译为

$$c(x)=1+x^2+x^4+x^6+x^7+x^8+x^{12}+x^{13}+x^{14}$$

我们知道，上述二元双纠错狭义 BCH 码的生成多项式为

$$g(x)=m^{(1)}(x)m^{(3)}(x)=(x^4+x+1)(x^4+x^3+x^2+x+1)=x^8+x^7+x^6+x^4+1$$

因此上述码字为

$$c(x)=g(x)(1+x^2+x^6)$$

以下是 BCH 码小结。

BCH码的主要参数

码长 $n \leqslant q^m - 1$（$n = q^m - 1$ 称作本原 BCH 码）

首元指数 b（$b = 1$ 时称作狭义 BCH 码）

设计距离 δ

维数 $k = n - \deg g(x)$

BCH码的主要性质

（1）$GF(q)$ 上码长为 n 且设计距离为 δ 的 BCH 码之维数 $k \geqslant n - m(\delta - 1)$，最小距离 $d \geqslant \delta$；

（2）码长为 n 且设计距离为 $\delta = 2t + 1$ 的二元 BCH 码之维数 $k \geqslant n - mt$，最小距离 $d \geqslant \delta$；

（3）由（1），（2）可知，BCH 码的信息率较高；

（4）一般而言，BCH 码的真实最小距离 d 难求，但在特定的条件下，有可能解决这一问题；

（5）存在有效的译码方法。

第七章　重量分布与设计

§7.1　麦克威廉姆斯(Macwilliams)方程

在前面几章中，我们已经涉及到线性码的重量分布的问题。一般地说，计算码的重量分布是一项十分困难的任务。在一个大型计算机上，只能够在合理的时间内计算出一个中等大小的、诸如二元（40，20）码的重量分布。至于更大的码，则必须借助于理论上的成果和其它方面的知识了。尽管这是一个困难的问题，但由于它在理论上和实际应用中的重要性，例如用于计算码的正确译码概率等等，人们对这一问题进行了坚持不懈的研究，并得出一些重要的结果。

为了完整起见，我们把第六章中介绍过的定理6.7.5以另外一种形式写在这里。为此我们先引入下述定义。

定义7.1.1　设M_i为（n，k）码C中重量为i的码字（作为行）组成的矩阵。若对于任意重量i，M_i中的各列都具有相同的重量，则称C为**齐次码**。

这样一来，定理6.7.5可以写成（并加以适当扩充）如下形式，其证明是完全类似的。

定理7.1.1　设C为（n，k）齐次码。命$\{A_i\}$表示C的重量分布，$\{a_i\}$表示删除码的重量分布，则有

（1）　$a_i=\frac{n-i}{n}A_i+\frac{i+1}{n}A_{i+1}$

设B是C的一个子码，其中B的码字在某个固定坐标皆为零。命$\{b_i\}$表示B的重量分布，则有

（2）　$b_i=\frac{n-i}{n}A_i$

另一方面，设C中所有码字的重量都是偶数，则有

(3) $a_{2j-1}=\frac{2j}{n}A_{2j}$

(4) $a_{2j}=\frac{n-2j}{n}A_{2j}$

我们知道，如果一个码的自同构群是传递群，则该码是齐次码（参看定理6.7.8及其证明）。我们正是用这个条件来判定齐次码的。类似于二元扩展QR码，可以证明二元扩展 BCH 码的自同构群是传递群，因而任何二元 BCH 码的最小重量都是奇数。

在例2.7.2中，我们已经求出二元扩展（8，4，4）QR码的重量分布为

$$A_0=A_8=1，A_4=14$$

它的删除码，即（7，4，3）QR码的重量分布为

$$a_0=a_7=1，a_3=a_4=7$$

读者容易由此验证定理7.1.1的正确性。

关于重量分布的一个重要结果是所谓麦克威廉姆斯方程（简称麦氏方程），它将码C的重量分布与其对偶码$C^{\perp}$的重量分布联系起来。当C为自对偶码时，麦氏方程对C的重量分布加以很强的限制，我们往往可以由此获得C的重量分布。麦氏方程有多种证明方法，下面介绍的是一种初等证法。

引理7.1.1 设V为$GF(q)$上的向量空间，且U和W是V的子空间。于是，

$$q^{\dim(U\cap W)}=\frac{q^{\dim U}}{q^{\dim W^{\perp}}}q^{\dim(U^{\perp}\cap W^{\perp})} \tag{7-1}$$

证明 根据定理2.3.4，我们有

$$\begin{aligned} n &=\dim(U^{\perp}\cap W^{\perp})+\dim(U^{\perp}\cap W^{\perp})^{\perp} \\ &=\dim(U^{\perp}\cap W^{\perp})+\dim(U+W) \end{aligned}$$

因此

$$\begin{aligned} &\dim U+\dim(U^{\perp}\cap W^{\perp}) \\ &=\dim U+n-\dim(U+W) \end{aligned} \tag{7-2}$$

根据维数公式（定理2.1.7），我们有

$$\dim U+\dim W=\dim(U+W)+\dim(U\cap W)$$

因此

$$\begin{aligned}&\dim(U\cap W)+\dim W^{\perp}\\ &=\dim U+\dim W-\dim(U+W)+\dim W^{\perp}\\ &=\dim U+n-\dim(U+W)\end{aligned}\tag{7-3}$$

比较式（7-2）与式（7-3），得

$$\begin{aligned}&\dim U+\dim(U^{\perp}\cap W^{\perp})\\ &=\dim(U\cap W)+\dim W^{\perp}\end{aligned}\tag{7-4}$$

由于式（7-4）与式（7-1）等价，故引理得证。〈证毕〉

定理7.1.2 （麦氏定理） 设C为$GF(q)$上的(n, k)码。命$\{A_i\}$表示C的重量分布，$\{B_i\}$表示C的对偶码$C^{\perp}$的重量分布。于是

$$\sum_{j=0}^{n}\binom{j}{\nu}A_j=q^{k-\nu}\sum_{j=0}^{n}(-1)^j\gamma^{\nu-j}\binom{n-j}{n-\nu}B_j\tag{7-5}$$

$$\sum_{j=0}^{n}\binom{n-j}{n-\nu}B_j=q^{\nu-k}\sum_{j=0}^{n}\binom{n-j}{\nu}A_j\tag{7-6}$$

其中$\nu=0, 1, \cdots, n$，$\gamma=q-1$

证明 我们只证式（7-6）。式（7-5）的证明留给读者。

设S为坐标集合的一个子集，且$|S|=\nu$。因此在某个势为ν的坐标子集S上，C中为零的码字总数为

$$\binom{n}{\nu}A_0+\binom{n-1}{\nu}A_1+\binom{n-2}{\nu}A_2+\cdots+\binom{\nu}{\nu}A_{n-\nu}$$

$$=\sum_{j=0}^{n}\binom{n-j}{\nu}A_j$$

设U为n维向量V的子空间，其中U的向量在某个固定的势为ν的坐标子集S上为零。于是$\dim U=n-\nu$。显然，$U^{\perp}$也是V的子空间，其中$U^{\perp}$的向量在S以外的坐标上全为零，并且$\dim U^{\perp}=\nu$。综上所述，并在引理7.1.1中令$W=C$，我们有

$$\sum_{j=0}^{n}\binom{n-j}{\nu}A_j=\sum_{\nu\,;\ \dim U=n-\nu}q^{\dim(U\cap C)}$$

$$=q^{k-\nu}\sum_{\nu\,;\ \dim U^{\perp}=\nu}q^{\dim(U^{\perp}\cap C^{\perp})}$$

$$=q^{k-\nu}\sum_{S\,;\ |S|=\nu}$$ $C^{\perp}$ 中所有在S以外的坐标上为零的码字数目

$$=q^{k-\nu}\sum_{j=0}^{n}\binom{n-j}{n-\nu}B_j$$

〈证毕〉

上述定理中的式（7-5）和式（7-6）即称为麦氏方程，或麦氏等式。

麦氏方程还有另一种形式。实践证明，用重量计数器的多项式表示码C的重量分布往往是很方便的。我们称下述齐次多项式

$$W_C(x,\ y)=A_0x^n+A_1x^{n-1}y+A_2x^{n-2}y^2+\cdots+A_ny^n \qquad (7\text{-}7)$$

为码C的**重量计数器**。对于二元（n，k）码C，$|C|=2^k$。于是，上述麦氏等式可写为

$$W_{C^{\perp}}(x,\ y)=\frac{1}{|C|}W_C(x+y,\ x-y) \qquad (7\text{-}8)$$

或

$$\sum_{i=0}^{n}B_ix^{n-i}y^i=\frac{1}{|C|}\sum_{j=0}^{n}A_j(x+y)^{n-j}(x-y)^j \qquad (7\text{-}9)$$

我们分别用$\{A_j\}$和$\{B_j\}$表示码C和$C^{\perp}$的重量分布。

通过直接验证，即可证明麦氏等式与式（7-8）或式（7-9）等价。例如，当$\nu=0$时，由式（7-6）可得

$$B_0=\frac{1}{2^k}\sum_{j=0}^{n}A_j$$

我们知道，B_0是式（7-9）左边x^n项的系数，而$\frac{1}{|C|}\sum_{j=0}^{n}A_j$则是

式（7-9）右边x^n项的系数。因此，式（7-9）关于x^n项的系数是正确的。如此继续下去，可以证明式（7-9）关于x^i项（$i=0$，1，…，n）的系数全部正确。

例7.1.1 设（2，1）码C为

$$\{00,\ 11\}$$

则显然有

$$C^{\perp}=\{00,\ 11\}=C$$

故C为自对偶码，并且

$$W_C=x^2+y^2$$

由式（7-8）可得

$$\frac{1}{2}W_C(x+y,\ x-y)=\frac{1}{2}[(x+y)^2+(x-y)^2]$$

$$=x^2+y^2=W_C(x,\ y)$$

因为C是自对偶码，所以上述结果$W_{C^{\perp}}(x,\ y)=W_C(x,\ y)$是正确的。

例7.1.2 设C为二元（7，4，3）汉明码。

$$A_0=A_7=1,\quad A_3=A_4=7$$

我们也知道，$C^{\perp}$是C的偶重量子码，因此

$$B_0=1,\quad B_4=7$$

于是C和$C^{\perp}$的重量计数器分别为

$$W_C=x^7+7x^4y^3+7x^3y^4+y^7$$

$$W_{C^{\perp}}=x^7+7x^3y^4$$

根据式（7-8），有

$$\frac{1}{16}W_C(x+y,\ x-y)$$

$$=\frac{1}{16}[(x+y)^7+7(x+y)^4(x-y)^3+7(x+y)^3(x-y)^4+(x-y)^7]$$

$$=\frac{1}{16}\left[2\left(x^7+\binom{7}{2}x^5y^2+\binom{7}{4}x^3y^4+\binom{7}{6}xy^6\right)\right.$$

$$+14(x^2-y^2)^3x\Big]$$

$$=\frac{1}{8}[x^7+21x^5y^2+35x^3y^4+7xy^6+7x^7$$

$$-21x^5y^2+21x^3y^4-7xy^6]$$

$$=x^7+7x^3y^4=W_{C^\perp}(x,y)$$

这一结论与已知结果相符。

鉴于式（7-8）和式（7-9）与麦氏等式等价，我们也常称之为麦氏等式。

最后我们作一个注记。麦氏等式（7-8）关于C和$C^\perp$是对称的，亦即有

$$W_C(x,y)=\frac{1}{|C^\perp|}W_{C^\perp}(x+y,x-y) \quad (7\text{-}10)$$

事实上，令

$$u=x+y,\quad v=x-y$$

则有

$$x=\frac{1}{2}(u+v),\ y=\frac{1}{2}(u-v)$$

代入式（7-9），得

$$\frac{1}{2^n}\sum_{i=0}^{n}B_i(u+v)^{n-i}(u-v)^i$$

$$=\frac{1}{|C|}\sum_{j=0}^{n}A_ju^{n-j}v^j$$

因为$|C|=2^k$，$|C^\perp|=2^{n-k}$，所以

$$|C|\cdot|C^\perp|=2^n$$

因此式（7-10）成立。

§7.2 最大距离可分码和RS码

这一节，我们借讨论码的重量分布的时机，介绍最大距离可分码。这一类码之所以重要，因为它是在给定n和k之后，纠错

能力最强的（n，k）码。此外，它的特点是，重量分布是完全确定了的。

在§2.5中，我们已经知道，关于$GF(q)$上的（n,k,d）码C的辛格里通限是

$$d \leqslant n-k+1$$

当$d=n-k+1$时，C的码字之间达到了最大可能的距离。这时，称C为**最大距离可分码**，或简称为**MDS码**。关于可分码的含义，在讲了推论7.2.2.1之后自明。

以下，我们设$GF(q)$上的（n，k，d）码C的生成矩阵为G，一致校验矩阵为H。

定理7.2.1 C为MDS码当且仅当H中任意$n-k$列都线性无关。

证明 由推论2.5.4.1可知，对于码C而言，$d=n-k+1$，当且仅当H中任意$d-1=n-k$列都线性无关。 〈证毕〉

定理7.2.2 C为MDS码当且仅当$C^{\perp}$为MDS码。

证明 由于$C^{\perp\perp}=C$，我们只需证必要性。因为H为$C^{\perp}$的生成矩阵，由定理7.2.1可知，H中任意$n-k$列都线性无关，故只有零向量才能在$n-k$个坐标位上为零。因此$C^{\perp}$的最小距离$\geqslant k+1=n-(n-k)+1$。于是$C^{\perp}$为（n，$n-k$，$k+1$）MDS码。 〈证毕〉

推论7.2.2.1 下述3个命题是彼此等价的：

（1）C为MDS码；

（2）G中任意k列都线性独立（即码字中任意k位都可以取作信息位）；

（3）H中任意$n-k$列都线性独立。

证明 由定理7.2.1和定理7.2.2即得。

由推论7.2.2.1可知，MDS码的码字可以分为信息位和校验位。这就是可分码这一名称的由来。

定理7.2.3 （n，k，d）码C为MDS码当且仅当C在任意d个坐标上都有一个重量为d的码字。

证明 设C为MDS码。任意给定一个坐标集合的子集S，其中$|S|=d=n-k+1$。由推论7.2.2.1，我们可以取S中的一个坐标位和其余不属于S的$k-1$个坐标位为信息位。命S中选定的那个坐标为1，其余$k-1$个坐标为0，就得到一个重量为$d=n-k+1$的码字。读者不难证明，定理的充分性也成立。

〈证毕〉

推论7.2.3.1 设C为$GF(q)$上的(n, k, d)MDS码，则C中重量为$d=n-k+1$的码字总数为

$$(q-1)\binom{n}{d}=(q-1)\binom{n}{k-1} \tag{7-11}$$

证明 在定理7.2.3的证明中，我们可以命S中选定的坐标为$GF(q)$中的任意一个非零元素，故共有$q-1$种不同的取法。此外势为d的坐标子集合S共有$\binom{n}{d}$个。因此推论得证。

〈证毕〉

关于MDS码的重量分布，我们有下面的重要定理。

定理7.2.4 设C为$GF(q)$上的$(n, k, d=n-k+1)$MDS码，$\{A_i\}$为C的重量分布。于是

$$A_j=\binom{n}{j}\sum_{h=0}^{j-d}(-1)^h\binom{j}{h}(q^{j-d+1-h}-1) \tag{7-12}$$

证明 由麦氏等式（7-6），我们有

$$\sum_{j=0}^{n}\binom{n-j}{\nu}A_j=q^{k-\nu}\sum_{j=0}^{n}\binom{n-j}{n-\nu}B_j \tag{7-13}$$

$$\nu=0, 1, 2, \cdots, n$$

注意到

$$\binom{n}{m}=0\text{，对一切 } n<m$$

故式（7-13）可以改写为

$$\sum_{j=0}^{n-\nu}\binom{n-j}{\nu}A_j=q^{k-\nu}\sum_{j=0}^{\nu}\binom{n-j}{n-\nu}B_j \tag{7-14}$$

对于（n，k，$n-k+1$）MDS码C，我们有

$$A_j=0\text{，对一切 }1\leqslant j\leqslant n-k \tag{7-15}$$

类似地，根据定理7.2.2，我们知道$C^{\perp}$是（n，$n-k$，$k+1$）MDS码，因此

$$B_j=0\text{，对一切 }1\leqslant j\leqslant k \tag{7-16}$$

将式（7-15）代入式（7-14），则式（7-14）的左边为

$$\binom{n}{\nu}A_0+\sum_{j=n-k+1}^{n-\nu}\binom{n-j}{\nu}A_j \tag{7-17}$$

注意到在式（7-17）中，当$\nu\geqslant k$时，有$\binom{n-j}{\nu}=0$，故我们总假设

$$\nu=0\text{，}1\text{，}2\text{，}\cdots k-1 \tag{7-18}$$

将式（7-16）代入式（7-14），则式（7-14）的右边为

$$q^{k-\nu}\left[\binom{n}{n-\nu}B_0+\sum_{j=k+1}^{\nu}\binom{n-j}{n-\nu}B_j\right] \tag{7-19}$$

注意到式（7-18），故式（7-19）为

$$q^{k-\nu}\binom{n}{\nu}B_0 \tag{7-20}$$

结合式（7-17）和式（7-20），并由$A_0=B_0=1$，我们有

$$\sum_{j=n-k+1}^{n-\nu}\binom{n-j}{\nu}A_j=\binom{n}{\nu}(q^{k-\nu}-1) \tag{7-21}$$

$$\nu=0\text{，}1\text{，}2\text{，}\cdots\text{，}k-1$$

在式（7-21）中，令$\nu=k-1$，有

$$A_{n-k+1}=\binom{n}{k-1}(q-1) \tag{7-22}$$

在式（7-21）中，令$\nu=k-2$，有

$$\binom{k-1}{k-2}A_{n-k+1}+A_{n-k+2}=\binom{n}{k-2}(q^2-1)$$

将式（7-22）代入上式，得

$$A_{n-k+2}=\binom{n}{k-2}[(q^2-1)-(n-k+2)(q-1)] \tag{7-23}$$

我们不难证明

$$A_{n-k+r}=\binom{n}{k-r}\sum_{h=0}^{r-1}(-1)^h\binom{n-k+r}{h}(q^{r-h}-1) \tag{7-24}$$

令 $j=n-k+r$，则有

$$k-r=n-j$$
$$r-1=j-(n-k+1)=j-d$$
$$r-h=j-d+1-h$$

将上述结果代入式（7-24），即得

$$A_j=\binom{n}{j}\sum_{h=0}^{j-d}(-1)^h\binom{j}{h}(q^{j-d+1-h}-1)$$

此即式（7-12）。〈证毕〉

例7.2.1 已知存在$GF(8)$上的（8，4；5）MDS码C，则由式（7-12）可知

$$A_5=\binom{8}{5}(8-1)=\binom{8}{3}\times 7=392$$

$$A_6=\binom{8}{6}\left[(8^2-1)-\binom{6}{1}(8-1)\right]$$

$$=\binom{8}{2}(63-42)=28\times 21=588$$

$$A_7=\binom{8}{7}\left[(8^3-1)-\binom{7}{1}(8^2-1)+\binom{7}{2}(8-1)\right]$$
$$=8\times 217=1736$$
$$A_8=\binom{8}{8}\left[(8^4-1)-\binom{8}{1}(8^3-1)+\binom{8}{2}(8^2-1)\right.$$
$$\left.-\binom{8}{3}(8-1)\right]=4095-4088+1764-392=1379$$

此外还有

$$A_0=1,\quad A_1=A_2=A_3=A_4=0$$

注意

$$\sum_{j=0}^{8}A_j=q^k=8^4=4096$$

定理7.2.4有下述重要的推论。

推论7.2.4.1 设C为$GF(q)$上的$(n,\ k,\ n-k+1)$ MDS码。于是

（1）若$k\geqslant 2$，则$q\geqslant n-k+1$ $\qquad$ (7-25)

（2）若$k\leqslant n-2$，则$q\geqslant k+1$ $\qquad$ (7-26)

证明 （1）由式(7-23)，我们有

$$A_{n-k+2}=\binom{n}{k-2}[(q^2-1)-(n-k+2)(q-1)]$$
$$=\binom{n}{k-2}(q-1)(q-n+k-1)$$

由于$A_{n-k+2}\geqslant 0$，故当$k\geqslant 2$时，有

$$q-n+k-1\geqslant 0$$

或

$$q\geqslant n-k+1$$

（2）考虑$C^{\perp}$的重量分布。将（1）中的k换成$n-k$便有当$n-k\geqslant 2$，即$k\leqslant n-2$时，则有$q\geqslant k+1$。

（证毕）

特别，当 $q=2$ 时，式（7-25）与式（7-26）分别为

若 $k \geqslant 2$，则 $d \leqslant 2$

若 $d \geqslant 3$，则 $k \leqslant 1$

由此可见，二元 MDS码只有两类：即 $k=1$ 时的二元重复码和 $d=2$ 时的平凡情形（有时也称作单一致校验码）。

当 $q>2$ 时，非平凡的 MDS码是存在的.其中最著名的是里德—所罗门（Reed—Solomon）码，简称为 RS 码.

定义7.2.1 设 $q>2$，我们称 $GF(q)$ 上码长为 $n=q-1$ 的 BCH 码为 RS 码。

设 α 为 $GF(q)$ 中的本原域元素。由于

$$x^{q-1}-1=\prod_{\substack{\beta \in GF(q) \\ \beta \neq 0}}(x-\beta)$$

故 α^i 的最小多项式为 $m^{(i)}(x)=x-\alpha^i$。因此，码长为 $n=q-1$ 且设计距离为 δ 的 RS码的生成多项式为

$$g(x)=(x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+\delta-2}) \qquad (7\text{-}27)$$

通常，取 $b=1$。

根据BCH码的已知结果，我们不难求出RS 码 C 的维数 k 和最小距离 d。显然有

$$\dim C=k=n-\deg g(x)=n-\delta+1 \qquad (7\text{-}28)$$

因此，

$$\delta=n-k+1$$

由定理6.9.2(BCH 限）可知，

$$d \geqslant \delta=n-k+1$$

再由定理2.5.7(辛格里通限）得

$$d=\delta=n-k+1 \qquad (7\text{-}29)$$

由此可见RS 码是 MDS 码。因此我们前面讲过的有关 MDS 码的结论（特别是定理7.2.4）对RS码都适用。

RS码是一类特殊的 BDH 码，它本身也具有重要意义。第一，当所求码长小于域的大小时，RS码最为适用。因为作为 MDS码，

它的纠错能力是最强的；第二，RS 码可以用来构造其它码类，例如级连码；第三，RS 码不但可以纠正随机错误，还可以纠正突发错误。

例7.2.2 考虑由 $\alpha^2+\alpha+1=0$ 定义的有限域 $GF(4)=\{0, 1, \alpha, \alpha^2=\beta\}$。于是，$GF(4)$ 上码长为 $n=3$、设计距离为 $\delta=2$ 的 $(3, 2, 2)$RS 码 C 的生成多项式为

$$g(x)=x-\alpha$$

它的一个生成矩阵为

$$G=\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \end{pmatrix}$$

由此可以得出 C 的全部 $4^2=16$ 个码字

$$\begin{array}{cccc} 0\,0\,0 & \alpha\,1\,0 & \beta\,\alpha\,0 & 1\,\beta\,0 \\ 0\,\alpha\,1 & \alpha\,\beta\,1 & \beta\,0\,1 & 1\,1\,1 \\ 0\,\beta\,\alpha & \alpha\,\alpha\,\alpha & \beta\,1\,\alpha & 1\,0\,\alpha \\ 0\,1\,\beta & \alpha\,0\,\beta & \beta\,\beta\,\beta & 1\,\alpha\,\beta \end{array}$$

C 的另一个生成矩阵是

$$G'=\begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & \beta \end{pmatrix}$$

故 $C^{\perp}$ 的一个生成矩阵为

$$G^{\perp}=(\alpha \quad \beta \quad 1)$$

因此 $C^{\perp}$ 的全部 4 个码字为

$$\begin{array}{ccc} 0 & 0 & 0 \\ \alpha & \beta & 1 \\ \beta & 1 & \alpha \\ 1 & \alpha & \beta \end{array}$$

由此可见，$C^{\perp}$ 是 $(3, 1, 3)$MDS 码。不仅如此，$C^{\perp}$ 也是 $GF(4)$ 上的RS码，其生成多项式为

$$g^{\perp}(x)=(x+\alpha^0)(x+\alpha)=(x+1)(x+\alpha)$$

一般地，我们可以证明，RS码的对偶码也是 RS 码。这一性

质是一般的BCH码所没有的。

回到我们这个例题，利用定理7.2.4，可以计算出

$$A_0=1,\ A_1=0$$

$$A_2=\binom{3}{2}(4-1)=9$$

$$A_3=\binom{3}{3}\left[(4^2-1)-\binom{3}{1}(4-1)\right]=(15-9)=6$$

显然有

$$A_0+A_1+A_2+A_3=16=4^2$$

类似地，我们也可以通过定理7.2.4计算出$C^{\perp}$的重量分布为

$$B_0=1,\ B_1=B_2=0$$

$$B_3=3$$

最后我们对RS码作一小结。

RS 码小结

基本参数

码长：$n=q-1$

设计距离：δ

维数：$k=n-\delta+1$

最小距离：$d=\delta=n-k+1$

主要性质

（1）设α为$GF(q)$中的本原域元素。RS码是循环码，其生成多项式为

$$g(x)=(x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+\delta-2})$$

通常，取$b=1$。

（2）RS 码是BCH码。

（3）RS 码是MDS码。

（4）RS码的重量分布是完全确定的。

（5）RS码可以纠正突发错误。

(6) RS码可用于构造其它码类，例如级连码。

§7.3 普列斯(Pless)幂矩

为了讨论与麦氏等式等价的普列斯幂矩等式，我们需要作一些准备。

定义7.3.1 设 $r \geqslant \nu \geqslant 0$，将 r 个不同的物体放到 ν 个相同的盒子中，且无一空盒的方法总数称作**第二类斯特林(Stirling)数**，记作 $S(r, \nu)$。

例如，将 a、b、c 三个物体放到两个相同的盒子中，且不允许空盒的放法有三种，如表7-1所示。

表 7-1

	放法 1	放法 2	放法 3
盒 1	a	b	c
盒 2	bc	ac	ab

因此 $S(3, 2)=3$。

关于第二类斯特林数，有许多性质与公式。我们不加证明地给出其中一部分。

定理7.3.1 对于第二类斯特林数 $S(r, \nu)$，我们有

(1) $S(0, 0)=1$

$$S(r, 0)=0, \text{ 对一切 } r \neq 0$$

$$S(r, 1)=S(r, r)=1$$

$$S(r, 2)=2^{r-1}-1$$

$$S(r, r-1)=\binom{r}{2}$$

(2) $$S(r, \nu)=\frac{1}{\nu!}\sum_{i=0}^{\nu}(-1)^{\nu-i}\binom{\nu}{i}i^r \qquad (7\text{-}30)$$

（3）（递推公式） 设 $r \geqslant \nu \geqslant 1$，则有

$$S(r+1,\ \nu)=\nu S(r,\ \nu)+S(r,\ \nu-1) \quad (7\text{-}31)$$

$$（4）\ (n-j)^r=\sum_{\nu=0}^{r} \nu!\binom{n-j}{\nu}S(r,\ \nu) \quad (7\text{-}32)$$

通过初始条件和递推公式，不难得到某些第二类斯特林数（见表7-2）。

表 7-2

r \ ν	1	2	3	4	5	6	7
1	1						
2	1	1					
3	1	3	1				
4	1	7	6	1			
5	1	15	25	10	1		
6	1	31	90	65	15	1	
7	1	63	301	350	140	21	1

现在，我们有条件讨论普列斯幂矩了。

定理7.3.2 （普列斯幂矩定理）

设 C 为 $GF(q)$ 上的 $(n,\ k)$ 码，且 $\gamma=q-1$。命 $\{A_j\}$ 和 $\{B_j\}$ 分别表示 C 与 $C^{\perp}$ 的重量分布。于是下列普列斯幂矩等式成立：

$$\sum_{j=0}^{n} j^r A_j$$

$$=\sum_{j=0}^{n}(-1)^j B_j\sum_{\nu=0}^{r}\nu!\,S(r,\ \nu)q^{k-\nu}\gamma^{\nu-j}\binom{n-j}{n-\nu} \quad (7\text{-}33)$$

$$\sum_{j=0}^{n}(n-j)^r A_j$$

$$=\sum_{j=0}^{n}B_j\sum_{\nu=0}^{r}\nu!\,S(r,\ \nu)q^{k-\nu}\binom{n-j}{n-\nu} \quad (7\text{-}34)$$

由于 $r=0, 1, 2, \cdots$，故由式（7-33）或式（7-34）可以得到无限多个方程。如果我们约定 $\binom{u}{v}=0$，对一切 $v<0$，则当 $r>n$ 时，式（7-33）和式（7-34）仍然有意义。当 $r<n$ 时，显然式（7-33）和式（7-34）右边的 $\sum_{j=0}^{n}$ 可代之以 $\sum_{j=0}^{r}$。当 $q=2$ 时，$\gamma=1$。

证明 我们证明，由麦氏等式（7-6）可以推导出普列斯幂矩等式（7-34）。类似地，由式（7-5）可以推导出式（7-33）。

由式（7-32）可得

$$\sum_{j=0}^{n}(n-j)^r A_j=\sum_{j=0}^{n}\left(\sum_{\nu=0}^{r}\nu!\binom{n-j}{\nu}S(r,\ \nu)\right)A_j$$

$$=\sum_{\nu=0}^{r}\nu!S(r,\ \nu)\sum_{j=0}^{n}\binom{n-j}{\nu}A_j$$

$$=\sum_{\nu=0}^{r}\nu!S(r,\ \nu)\sum_{j=0}^{n}q^{k-\nu}\binom{n-j}{n-\nu}B_j$$

$$=\sum_{j=0}^{n}B_j\sum_{\nu=0}^{r}\nu!S(r,\ \nu)q^{k-\nu}\binom{n-j}{n-\nu}$$

反过来我们也可以由普列斯幂矩等式推导出麦氏等式。

（证毕）

有时也将麦氏等式称作麦氏二项式矩等式。

下面我们计算当 $q=2$ 时，式（7-33）中的前几个方程。

当 $r=0$ 时，有

$$\sum_{j=0}^{n}A_j=B_0\left(0!S(0,\ 0)2^k\binom{n}{n}\right)=2^k \tag{7-35}$$

当 $r=1$ 时，有

$$\sum_{j=0}^{n} jA_j = B_0\left(0!S(1,0)2^k\binom{n}{n} + 1!S(1,1)2^{k-1}\binom{n}{n-1}\right) - B_1\left(1!S(1,1)2^{k-1}\binom{n-1}{n-1}\right)$$

$$= 2^{k-1}n - 2^{k-1}B_1 \tag{7-36}$$

当 $r=2$ 时，有

$$\sum_{j=0}^{n} j^2A_j = B_0\left(0!S(2,0)2^k\binom{n}{n} + 1!S(2,1)2^{k-1}\binom{n}{n-1} + 2!S(2,2)2^{k-2}\binom{n}{n-2}\right)$$

$$-B_1\left(1!S(2,1)2^{k-1}\binom{n-1}{n-1} + 2!S(2,2)2^{k-2}\binom{n-1}{n-2}\right) + B_2\left(2!S(2,2)2^{k-2}\binom{n-2}{n-2}\right)$$

$$= 2^{k-2}n(n+1) - 2!2^{k-2}nB_1 + 2!2^{k-2}B_2 \tag{7-37}$$

类似地，当 $r=3$ 时，有

$$\sum_{j=0}^{n} j^3A_j = 2^{k-3}(n^3+3n^2) - 2^{k-3}(3n^2+3n-2)B_1$$

$$+ 3!2^{k-3}nB_2 - 3!2^{k-3}B_3 \tag{7-38}$$

当 $r=4$ 时，有

$$\sum_{j=0}^{n} j^4A_j = 2^{k-4}(n^4+6n^3+3n^2-2n)$$

$$-2^{k-2}(n^3+3n^2-9n+7)B_1 + 2^{k-2}(3n^2+3n-4)B_2$$

$$-4!2^{k-4}nB_3 + 4!2^{k-4}B_4 \tag{7-39}$$

我们提醒读者注意，任意码C的重量分布都必须满足麦氏方程和普氏恒矩。但是这些方程的一个解可能不是任何码的重量分布。例如，一个含有负数的解，就不可能是一个码的重量分布。

然而即使正整数解也未必是一个码的重量分布。因为我们只对作为码的重量分布的解感兴趣，故我们总是假定

$$A_0=B_0=1$$

普氏幂矩和麦氏方程是等价的。但是普列斯幂矩等式有其独特的优点。

定理7.3.3 设已知B_1，B_2，…，，B_{s-1}，且仅有 s 个 A_j 为未知数。于是式（7-33）(从而式（7-34)，式（7-5）和式(7-6))存在唯一的解。

证明 在式（7-33）中，前 s 个方程有 s 个未知数，其系数矩阵的行列式为范德蒙德行列式。这个行列式不等于零，因此前 s 个方程中的未知数 A_j 有唯一的解。在后面的方程中，每增加一个方程，都恰好增加一个B_j，因而也有唯一的解。 〈证毕〉

例7.3.1 设$q=2$，$n=8$，$d=4$，且$C=C^{\perp}$。因此，我们有

$$A_0=B_0=1$$
$$A_1=B_1=0$$
$$A_2=B_2=0$$

于是式（7-33）中的前 3 个方程为

$$\left.\begin{aligned}&A_4+A_6+A_8=15\\&4A_4+6A_6+8A_8=64\\&4^2A_4+6^2A_6+8^2A_3=288\end{aligned}\right\}\tag{7-40}$$

式（7-40）的行列式为

$$D=\begin{vmatrix}1&1&1\\4&6&8\\4^2&6^2&8^2\end{vmatrix}$$

这是一个范德蒙德行列式，故$D\neq 0$，因此式(7-40)有唯一的解。我们可以解A_4，A_6和A_8。但是我们已经知道（8，4，4）汉明码的重量分布为

$$A_0=A_8=1$$
$$A_4=14\tag{7-41}$$

因此

$$A_4=14,\quad A_6=0,\quad A_8=1$$

一定是式（7-40）的唯一解。

值得注意的是，尽管一种重量分布是唯一的，但并不等于说具有这种重量分布的码也是唯一的，亦即不等价的码有可能具有相同的重量分布。但是可以证明二元汉明（8， 4， 4）码是具有重量分布式（7-41）的唯一的码。换言之，任何具有重量分布式（7-41）的码都与二元汉明（8， 4， 4）码等价。

例7 3.2 从第六章中对二次剩余码的讨论，我们知道当 $p\equiv -1\pmod 8$ 时，二元$\left(p,\ \frac{p-1}{2}\right)QR$ 码C（即第六章中的Q_1'或Q_2'）有下述性质：

（1）$A_i=0$，除非 $i\equiv 0\pmod 4$；

（2）$C^{\perp}$也是QR码，且$C^{\perp}=C+\langle \boldsymbol{h}\rangle$；

（3）$B_i=0$，除非 $i\equiv 0$ 或 $3\pmod 4$；

（4）$C^{\perp}$的最小重量d为奇数，C的最小重量为$d+1$。因此C的最大重量为$p-d$；

（5）$d^2-d+1\geqslant p$。

当$p=7$，23，31或47时，上述条件使得有足够多的B_i为零，因此定理7.3.3中的条件得到满足。可以验证，我们由此得到的唯一解与这些码的已知的重量分布完全符合。

例如，考虑二元（23， 11， 8）QR码C。由于C的最大重量为$23-7=16$，因此C的所有可能的非零A_i为A_8，A_{12}和A_{16}，于是，式（7-33）中的前3个方程为

$$\left.\begin{aligned}&A_8+A_{12}+A_{16}=23\times 89\\&8A_8+12A_{12}+16A_{16}=2^{10}\times 23\\&8^2A_8+12^2A_{12}+16^2A_{16}=2^9\times 23\times 24\end{aligned}\right\}$$

解之可得

$$A_8=22\times 23=506$$

$$A_{12}=56\times 23=1288$$

$$A_{16}=11\times 23=253$$

由于$C^{\perp}=C+\langle h\rangle$，我们有

$$B_0=B_{23}=1$$
$$B_8=B_{15}=506$$
$$B_{11}=B_{12}=1288$$
$$B_7=B_{16}=253$$

这正是（23，12，7）二元戈莱码的重量分布。可以证明，具有上述重量分布的二元码与二元（23，12，7）戈莱码等价。

根据上述结果，易得扩展（24，12，8）戈莱码的重量分布为

$$\mathscr{A}_0=\mathscr{A}_{24}=1$$
$$\mathscr{A}_8=253+506=759$$
$$\mathscr{A}_{12}=1288+1288=2576$$
$$\mathscr{A}_{16}=253+506=759$$

同样地，可以证明具有以上重量分布的码与（24，12，8）戈莱码等价。

类似于$p=23$的情形，我们可以通过式（7-33）计算出$p=7$，31，47时的QR码C的重量分布。某些二元$\left(p,\ \frac{p-1}{2}\right)$ QR码的重量分布（$p\equiv-1\ (\mathrm{mod}\ 8)$）见表7-3。

表 7-3

A_i \ p	7	23	31	47
A_0	1	1	1	1
A_4	7			
A_8		22×23	15×31	
A_{12}		56×23	280×31	276×47
A_{16}		11×23	589×31	7590×47
A_{20}			168×31	49588×47
A_{24}			5×31	81720×47
A_{28}				35420×47
A_{32}				3795×47
A_{36}				92×47

§7.4 设　计

迄今我们已经看到代数学，特别是有限域的理论在编码中的重要作用。事实上，数学中的其它分支，例如组合学也在编码理论中有深远影响。从本节起，我们将对此作一简要的介绍。

设计是组合学中的重要概念，源于农业品种试验的设计。对于设计，或更准确地说 t 一设计的研究，一个很重要的问题是 t 一设计的存在性问题。例如，射影平面是 2 一设计。我们常将 t 一设计看成是射影平面的推广。所谓**射影平面**是点与线（或通称为区组，不一定是直线）的集合，并满足下述 4 条公理：

（1） 任意两点恰位于一条线上；

（2） 任意两线恰相交于一点；

（3） 任意一条线上至少含有 3 个点；

（4） 射影平面至少有 3 个点不在一条线上。

图 7-1 给出了一个最小射影平面（称为 2 阶射影平面）。后面我们知道，它构成一个 2 —（7， 3， 1）设计。现在，我们只注意到，该 2 阶射影平面有 7 个点，编号分别为

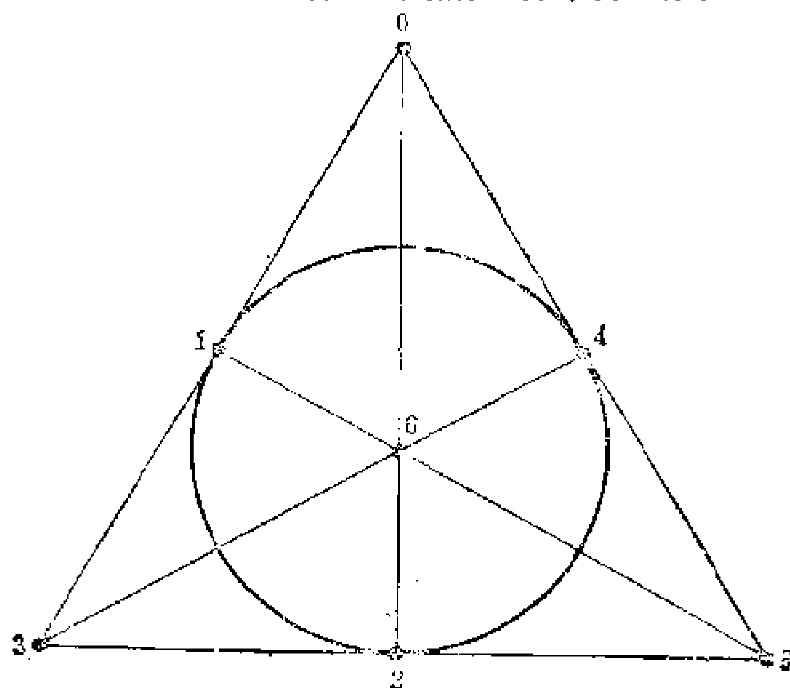

图 7-1

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$$

并有7条线，或7个区组，其中6条线是直线，一条线是弧线。它们是

B_0,	B_1,	B_2,	B_3,	B_4,	B_5,	B_6
013,	124,	235,	346,	450,	561,	602

其中区组B_0表示点0、1、3所在的直线，余此类推。我们还注意到，其中一条线上有3个点，一个点通过3条线，任意两个点恰属于一个区组。

定义7.4.1 设X为v—集合（即含有v个元素的集合），且将X中的元素称作点。t-(v, k, λ)设计由X和X的k—子集（称作区组）组成，并具有下述性质：X的任意t—子集都恰包含在λ个区组之中。特别，当$\lambda=1$时，t—设计称作**斯坦纳**(Steiner)**系统**，记作$S(t, k, v)$。

由定义可知，上述2阶射影平面是2—(7，3，1)设计，因而是斯坦纳系统$S(2, 3, 7)$。一般地，n阶射影平面是$S(2, n+1, n^2+n+1)(n\geqslant 2)$。此外还有，当$n\geqslant 2$时$n$阶仿射平面是$S(2, n, n^2)$。

定理7.4.1 t—(v, k, λ)设计也是i—(v, k, λ_i)设计，其中$1\leqslant i\leqslant t$。此外还有

$$\lambda_i=\frac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}}=\frac{\lambda(v-i)\cdots(v-t+1)}{(k-i)\cdots(k-t+1)} \qquad (7\text{-}42)$$

其中$0\leqslant i\leqslant t$。

证明 当$i=t$时，结论显然成立。我们只需证明，当$i=t-1$时，定理仍然成立。事实上，任意给定$t-1$个点。于是我们可以从$v-(t-1)$个点中任意选取1个，从而获得t个点。由t—设计的定义，任意t个点都恰好包含在λ个区组之中。另一方面，对于任意区组，在区组中选取额外的（即除给定

的 $t-1$ 个点以外的）一个点的方法共有 $k-(t-1)$ 种。因此

$$\lambda_{t-1}=\frac{\lambda(v-t+1)}{k-t+1}$$

（证毕）

推论7.4.1.1 设 $t-(v,\ k,\ \lambda)$ 设计中共有 b 个区组，于是

$$b=\frac{\lambda\binom{v}{t}}{\binom{k}{t}} \tag{7-43}$$

证明 由于含有 v 个点的集合 X 中共有 $\binom{v}{t}$ 个 t—子集，每一个 t—子集都恰属于 λ 个区组，并且在一个给定的区组中共有 $\binom{k}{t}$ 个 t—子集，因此式（7-43）成立。 （证毕）

推论7.4.1.2 在 $t-(v,\ k,\ \lambda)$ 设计中，设任意点都恰属于 r 个区组，于是

$$bk=vr \tag{7-44}$$

证明 由于 $r=\lambda_1$，故由定理 7.4.1 得

$$r=\frac{\lambda(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)} \tag{7-45}$$

另一方面

$$b=\frac{\lambda v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)} \tag{7-46}$$

比较式（7-45）及式（7-46）得

$$b=\frac{v}{k}r$$

即式（7-44）成立。 （证毕）

推论7.4.1.3 在 $2-(v,\ k,\ \lambda)$ 设计中，下式成立：

$$\lambda(v-1)=r(k-1) \tag{7-47}$$

证明 仍由定理7.4.1得

$$r=\frac{\lambda\binom{v-1}{1}}{\binom{k-1}{1}}=\frac{\lambda(v-1)}{k-1}$$

即式（7-47）成立。 （证毕）

推论7.4.1.4 t—（v，k，λ）设计存在的必要条件是

$$\lambda_i=\frac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$$

都是整数，其中$0\leqslant i\leqslant t$。

证明 显然。

注意，一般而言，上述条件并不充分。但在某些特殊情形，如对于斯坦纳系统$S(2,3,v)$、$S(2,4,v)$、$S(2,5,v)$，上述条件也是充分条件。

当$b=v$时，由推论7.4.1.2，我们知道$r=k$，此时称t—（v，k，λ）设计为**对称t—设计**。例如，2阶射影平面即为对称2—（7，3，1）设计。

定义7.4.2 给定一个有v个点P_1，…，P_v和b个区组B_1，…，B_b的t—（v，k，λ）设计，我们定义它的关联矩阵$A=\{a_{ij}\}$为

$$a_{ij}=\begin{cases}1, & 若\ P_j\in B_i\\ 0, & 若\ P_j\in B_i\end{cases}$$

显然A为$b\times v$矩阵。

今后我们将看到，关联矩阵是描述t—设计的一种有力工具。

例7.4.1 根据定义，2阶射影平面所构成的$2-(7,3,1)$设计的关联矩阵A为

$$
\begin{array}{c} \\ A= \end{array}
\begin{array}{c}
\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\
\hline
\begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}
\end{array}
\qquad (7-48)
$$

由式（7-48）可见

（1）A中每一行的重量均为3，说明2—设计中每个区组都含有3个点，即$k=3$；

（2）A中每一列的重量也是3，说明2—设计中每个点都恰属于3个不同的区组，亦即$r=3$；

（3）任意选定两个坐标i和j，其中$0\leqslant i<j\leqslant 6$，于是$A$中有且仅有一行在这两个坐标为1。这表明2—设计中任意两点都恰包含在$\lambda=1$个区组之中。

此外，由$b=v=7$，$k=r=3$，$\lambda=1$，$t=2$，容易验证$bk=vr$及$\lambda(v-1)=r(k-1)$等公式成立。

定义7.4.3 设P_1，P_2，…，P_t为t个固定点。对于$t\geqslant i\geqslant j\geqslant 0$，我们定义**区组相交数**$\lambda_{ij}$为包含点$P_1$，$P_2$，…，$P_j$，但不包含点$P_{j+1}$，$P_{j+2}$，…，$P_i$的区组的数目。

特别我们约定λ_{i0}为不包含点P_1，P_2，…，P_i的区组的数目，$\lambda_{00}=b$，且λ_{ii}为包含P_1，P_2，…，P_i的区组的数目。因此$\lambda_{ii}=\lambda_i$。

下面的定理告诉我们，区组相交数λ_{ij}的定义是合理的。

定理7.4.2 设$\mathscr{D}$为$t-(v,k,\lambda)$设计，且令$t\geqslant i\geqslant j\geqslant 0$。于是，区组相交数$\lambda_{ij}$的定义是合理的，即$\lambda_{ij}$与$i$个

点的选取方法无关。并且下式成立

$$\lambda_{(i-1)(j-1)}=\lambda_{ij}+\lambda_{i(j-1)} \tag{7-49}$$

最后当$\mathscr{D}$为斯坦纳系统$S(t, k, v)$时，$\lambda_{ii}=1$，对一切$k\geqslant i\geqslant t$；并且式（7-49）成立。

证明 由定义知，$\lambda_{ii}=\lambda_i$。因为$i\leqslant t$，故由定理7.4.1，$\mathscr{D}$为i设计，因此λ_{ii}与i个点的选择无关。若$i=0$，则$\lambda_{00}=b$。我们称$\lambda_{i'j'}$在λ_{ij}的前面，如果$i>i'$，或者$i=i'$，且$j'>j$。今设定理对所有在$\lambda_{i(j-1)}$前面的$\lambda_{i'j'}$都成立，我们证明定理对$\lambda_{i(j-1)}$也成立。显然$\lambda_{(i-1)(j-1)}$在λ_{ij}之前，而λ_{ij}又在$\lambda_{i(j-1)}$之前。现在我们选择i个点P_1，P_2，…，P_i。于是，$\lambda_{i(j-1)}$是包含P_1，…，P_{j-1}，但不包含P_j，…，P_i的区组的数目。由假设$\lambda_{(i-1)(j-1)}$和λ_{ij}都与这些点的选择无关。因此$\lambda_{(i-1)(j-1)}$是包含P_1，…，P_{j-1}，但不包含P_j，…，P_{i-1}的区组的数目；而λ_{ij}是包含P_1，…，P_{j-1}，P_i，但不包含P_j，…，P_{i-1}的区组的数目。因为包含P_1，…，P_{j-1}，但不包含P_j，…，P_{i-1}的区组既可能包含P_i，也可能不包含P_i，因此有

$$\lambda_{(i-1)(j-1)}=\lambda_{i(j-1)}+\lambda_{ij}$$

上述结果表明，对于任意$t-(v, k, \lambda)$设计，它的区组相交数λ_{ij}可以构成所谓"帕斯卡"(Pascal) 三角形

$$\begin{array}{c}\lambda_{00}=b\\ \lambda_{10}\qquad \lambda_{11}=\lambda_1\\ \lambda_{20}\quad \lambda_{21}\qquad \lambda_{22}=\lambda_2\\ \lambda_{30}\quad \lambda_{31}\quad \lambda_{32}\qquad \lambda_{33}=\lambda_3\\ \cdots\end{array}$$

并且可以下述次序计算。这个三角形的顶点$\lambda_{00}=b$，然后计算$\lambda_{11}=\lambda_1$，再由λ_{11}和λ_{00}可以求出λ_{10}。一般地，当计算出第i行后，就计算$\lambda_{(i+1)(i+1)}$，然后可以由右到左地逐步求出全部的$\lambda_{(i+1)j}$。

当$\mathscr{D}$为斯坦纳系统$S(t, k, v)$时，上述帕斯卡三角形可以扩展到第k级（习惯上，称帕斯卡三角形的第i行为第i

级）。由于 t 个点可以确定唯一的一个区组，故当 $k\geqslant i\geqslant t$ 时，有 $\lambda_{ii}=1$。又因帕斯卡三角形中的第 i 行可以通过 λ_{ii} 和前一行的结果计算出来，故定理的其余部分也成立。（证毕）

例如，对于2阶射影平面 $S(2, 3, 7)$，我们可以得到如下的3级（由于 $t=2$，$k=3$，我们将帕斯卡三角形扩展了1级）帕斯卡三角形

			7				0级
		4		3			1级
	2		2		1		2级
0		2		0		1	3级

注意上述帕斯卡三角形中的最后一行表明，选定某个区组的3个点 P_1，P_2 和 P_3 之后，可以断定包含这3个点的区组有一个（$\lambda_{33}=1$）；不包含这3个点的区组有0个（$\lambda_{30}=0$）；包含其中一个点（例如 P_1）但不包含其余两个点（例如 P_2 和 P_3）的区组有2个（$\lambda_{31}=2$）；包含其中两个点（例如 P_1 和 P_2）但不包含其余的点（例如 P_3）的区组有0个（$\lambda_{32}=0$）。这就是区组相交数名称的由来。读者不难通过关联矩阵式（7-48）直接验证上述结果。

给定一个 $t-(v, k, \lambda)$ 设计，可以“诱导出”若干别的设计，例如

定理7.4.3 设 $\mathscr{D}$ 为 $t-(v, k, \lambda)$ 设计，设 $\mathscr{D}_1$ 中的区组为 $\mathscr{D}$ 中包含一个固定点，并去掉该点后的全体区组。于是 $\mathscr{D}_1$ 是 $(t-1)-(v-1, k-1, \lambda)$ 设计，并称为“**导出设计**”。

证明 由 $\mathscr{D}$ 的帕斯卡三角形可以证明本定理。事实上，$\mathscr{D}_1$ 的帕斯卡三角形的顶点位于 λ_{11}，它的第一行为 λ_{21}，λ_{22}，…，总之 $\mathscr{D}_1$ 的帕斯卡三角形是由 $\mathscr{D}$ 的帕斯卡三角形去掉左边后所得到的三角形，从而定理得证。（证毕）

定理7.4.4 设 $\mathscr{D}$ 为 $t-(v, k, \lambda)$ 设计，且 $v-k\geqslant t$。令 $\mathscr{D}'$ 中的区组为 $\mathscr{D}$ 中区组之补。于是 $\mathscr{D}'$ 为 $t-(v, v-k,$

λ'）设计，其中

$$\lambda' = \frac{\lambda\binom{v-k}{t}}{\binom{k}{t}} \tag{7-50}$$

并称$\mathscr{D}'$为$\mathscr{D}$的补设计。

证明 因为$\lambda'=\lambda_{t0}$与t一子集的选择无关，故由区组相交数可见$\mathscr{D}'$为t—设计。由于$\mathscr{D}$和$\mathscr{D}'$的区组数均为b，故由推论7.4.1.1可知

$$b = \frac{\lambda\binom{v}{t}}{\binom{k}{t}} = \frac{\lambda'\binom{v}{t}}{\binom{v-k}{t}}$$

因此

$$\lambda' = \frac{\lambda\binom{v-k}{t}}{\binom{k}{t}}$$

《证毕》

例7.4.2

图7-2(a）为2阶射影平面2—(7，3，1）设计$\mathscr{D}$。设$\mathscr{D}$中的固定点为0，则$\mathscr{D}$的导出设计$\mathscr{D}'$为1—(6，2，1）设计，如图7-2(b）所示。

如果将$\mathscr{D}$视为斯坦纳系统S(2，3，7)，则$\mathscr{D}'$为斯坦纳系统S(1，2，6)。一般地，我们有

推论7.4.3 如果S(t，k，v）存在，则S($t-1$，$k-1$，$v-1$）也存在。

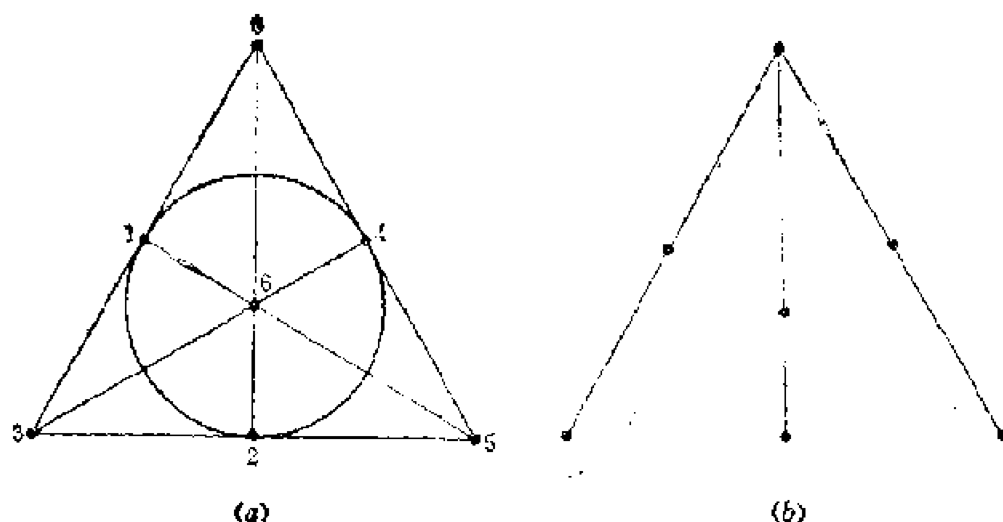

图 7-2

证明 由定理7.4.3即得。

$\mathscr{D}$和$\mathscr{D}'$的帕斯卡三角形分别为

$$\begin{matrix} & & & 7 & & & \\ & & 4 & & 3 & & \\ & 2 & & 2 & & 1 & \\ 0 & & 2 & & 0 & & 1 \end{matrix} \qquad\qquad \begin{matrix} & & 3 & & \\ & 2 & & 1 & \\ 2 & & 0 & & 1 \end{matrix}$$

$\mathscr{D}$的帕斯卡三角形 $\mathscr{D}'$的帕斯卡三角形

例7.4.3 设$\mathscr{D}$的定义如上例，则$\mathscr{D}$的补设计$\mathscr{D}'$含有下述$b=7$个区组：

$b_0=\{2,4,5,6\}$, $b_1=\{0,3,5,6\}$

$b_2=\{0,1,4,6\}$, $b_3=\{0,1,2,5\}$

$b_4=\{1,2,3,6\}$, $b_5=\{0,2,3,4\}$

$b_6=\{1,3,4,5\}$

由于

$$\lambda'=\frac{\binom{4}{2}}{\binom{3}{2}}=2$$

故$\mathscr{D}'$为2—(7，4，2）设计。这一点由下述$\mathscr{D}'$的关联矩阵

A' 看得很清楚：

$$
\begin{array}{c} \\ A' = \end{array}
\begin{array}{ccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
\end{array}
$$

$$
A' = \begin{pmatrix}
0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 0
\end{pmatrix} \qquad (7\text{-}51)
$$

比较式（7-48）与式（7-51）可见，A' 中的 1 为 A 中的 0，而 A' 中的 0 为 A 中的 1。

§7.5 设 计 和 码

设计与码之间有着密切的联系。t—(v，k，λ）设计的每一个区组都与关联矩阵 A 中的一个行相对应。我们可以把这些行看成是一个码中的码字。由于 A 中任意行都含有 k 个点，故关联矩阵 A 中的每一行都对应码中具有重量 k 的码字。我们称码长为 n 的二元码中具有重量 W 的码字**构成 t—设计**，如果这些码字是含有 n 个点的 t—设计中的区组。显然并非码中重量为 W 的码字一定构成 t—设计。

表 7-4

区组 \ 点	0	1	2	3	4	5	6
0	1	1	0	1	0	0	0
1	0	1	1	0	1	0	0
2	0	0	1	1	0	1	0
3	0	0	0	1	1	0	1
4	1	0	0	0	1	1	0
5	0	1	0	0	0	1	1
6	1	0	1	0	0	0	1

(7-52)

例如，表 7-4 的行作为循环码的二元（7，4，3）汉明码的 7 个重量为 3 的向量。比较式（7-52）与式（7-48）可知，这正是 2 —（7，3，1）设计的关联矩阵。因此，（7，4，3）二元汉明码中重量为 3 的向量构成 2 —（7，3，1）设计，或斯坦纳系统 $S(2, 3, 7)$。

鉴于关联矩阵的重要性，我们给出它的若干性质。

定理7.5.1 设 A 为 t —（v，k，λ）设计的 $b\times v$ 关联矩阵，且 λ_2 与 r 的定义均如前。命 I 为 $v\times v$ 单位矩阵，且 J 为所有阵元皆为 1 的 $v\times v$ 矩阵。于是

$$A'A=(r-\lambda_2)I+\lambda_2 J \tag{7-53}$$

证明 命 $R=A'A=(r_{ij})$，则 r_{ij} 为 A 的第 i 列与第 j 列的内积。因此当 $i\neq j$ 时，r_{ij} 表示 A 的第 i 列和第 j 列中对应分量都为 1 的数目，即 $r_{ij}=\lambda_2$。当 $i=j$ 时，r_{ii} 表示 A 的 i 列中 1 的数目，即 $r_{ii}=r$。由此可见

$$A'A=\begin{pmatrix} r & \lambda_2\cdots\lambda_2 \\ \lambda_2 & r\cdots\lambda_2 \\ \vdots & \vdots\cdots\vdots \\ \lambda_2 & \lambda_2\cdots r \end{pmatrix}=(r-\lambda_2)I+\lambda_2 J$$

（证毕）

推论7.5.1.1 $\det(A'A)=(r-\lambda_2)^{v-1}(v\lambda_2-\lambda_2+r)$ (7-54)

证明 由式（7-53）得

$$\det(A'A)=\begin{vmatrix} r & \lambda_2 & \lambda_2\cdots\lambda_2 \\ \lambda_2 & r & \lambda_2\cdots\lambda_2 \\ \lambda_2 & \lambda_2 & r\cdots\lambda_2 \\ \vdots & \vdots & \vdots\cdots\vdots \\ \lambda_2 & \lambda_2 & \lambda_2\cdots r \end{vmatrix}$$

将行列式的 2 — v 列分别减去第 1 列，然后将行列式的 2 — v 行都加到第 1 行，则得

$$\det(A'A)=\begin{vmatrix} r & \lambda_2-r & \lambda_2-r & \cdots & \lambda_2-r \\ \lambda_2 & r-\lambda_2 & 0 & \cdots & 0 \\ \lambda_2 & 0 & r-\lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \lambda_2 & 0 & 0 & \cdots & r-\lambda_2 \end{vmatrix}$$

$$=\begin{vmatrix} r+(v-1)\lambda_2 & 0 & 0 & \cdots & 0 \\ \lambda_2 & r-\lambda_2 & 0 & \cdots & 0 \\ \lambda_2 & 0 & r-\lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \lambda_2 & 0 & 0 & \cdots & r-\lambda_2 \end{vmatrix}$$

$$=(r-\lambda_2)^{v-1}(v\lambda_2-\lambda_2+r)$$

（证毕）

推论7.5.1.2 （费舍尔（Fisher）不等式）

$$b\geqslant v \tag{7-55}$$

证明 我们只考虑 $r>\lambda_2$ 时的非平凡情形。此时，$\det(A'A)\neq 0$，因此

$$\text{rank}(A'A)=v$$

若 $b<v$，则有

$$\text{rank}\,A\leqslant b$$

但是

$$\text{rank}(A'A)\leqslant\text{rank}\,A$$

故得

$$b\geqslant v$$

（证毕）

我们所关心的是，在什么样的条件下，码中具有重量 W 的向量构成 t 一设计。下面的定理告诉我们，某些特定的码类一定包含 t 一设计。

定理7.5.2 设 C 为二元（n，k，d）完备码，则 C 中重量为 d 的码字构成斯坦纳系统 $S(t+1, d, n)$，其中 $t=(d-1)/2$。

证明 由于半径为 t 的码球互不相交，且覆盖整个空间，故

任意重量为 $t+1$ 的向量都在唯一的一个码球之中。由于 d 为奇数，故 $t=\frac{d-1}{2}$，因此重量为 $t+1$ 的向量所在码球的码字（即码球的中心）的重量一定是 d。 〈证毕〉

由此可见，我们现在有了一种在码中寻找设计的方法，亦即完备码中具有最小重量的码字构成设计。可惜的是，完备码的类型是很少的。

推论7.5.2.1 二元汉明（$n≜2^r-1$，$n-r$，3）码中重量为3的码字构成斯坦纳系统 $S(2, 3, 2^r-1)$。

证明 由定理7.5.2即得。

推论7.5.2.2 二元戈莱（23，12，7）码中重量为7的码字构成斯坦纳系统 $S(4, 7, 23)$。

证明 定理7.5.2的直接结果。

推论7.5.2.3 设 C 为二元（n，k，d）完备码，则有

$$A_d=\frac{\binom{n}{t+1}}{\binom{d}{t+1}} \tag{7-56}$$

证明 由于 $A_d=b$，故由推论7.4.1.1可得式（7-56）。

〈证毕〉

由上述推论，对于二元（23，12，7）戈莱码，可得

$$A_7=\frac{\binom{23}{4}}{\binom{7}{4}}=253$$

而对于二元（$n≜2^r-1$，$n-r$，3）汉明码，我们有

$$A_3=\frac{\binom{2^r-1}{2}}{\binom{3}{2}}=\frac{(2^r-1)(2^r-2)}{6}$$

特别对于二元（7，4，3）汉明码，可得

$$A_3=\frac{7\times 6}{6}=7$$

定理7.5.3 码长为n的二元t—纠错完备码存在的必要条件是

$$\frac{\binom{n-i}{t+1-i}}{\binom{2t+1-i}{t+1-i}}$$

必须全为整数，其中$1\leqslant i\leqslant t$。

证明 由定理7.4.1和定理7.5.2即得（注意$d=2t+1$）。

由此可见，除定理2.6.4之外，我们获得了完备码存在的另一个必要条件。可以将两者结合在一起应用。例如，在§2.6中，我们曾提出码长为$n=90$的二元双纠错完备码的存在性问题。虽然$n=90$，$t=2$满足定理2.6.4，但是在定理7.5.3中取$n=90$，$t=2$和$i=2$，我们有

$$\frac{\binom{n-i}{t+1-i}}{\binom{2t+1-i}{t+1-i}}=\frac{\binom{88}{1}}{\binom{3}{1}}=\frac{88}{3}$$

因此码长为$n=90$的二元双纠错完备码不可能存在。

对于非完备码，判断码中具有重量W的码字是否构成t—设计是一个十分困难的问题。下述阿斯姆斯-麦特松(Assmus-Mat-

tson）定理是在特定条件下解决这一问题的一个很有用的定理。

定理7.5.4 （阿斯姆斯—麦特松定理）设 C 为二元(n, k, d) 码，且 $0 < t < d$。令 $\{B_i\}$ 表示 C 的对偶码 $C^{\perp}$ 的重量分布，且令

$$s \triangleq |\{ i \mid B_i \neq 0 \text{ 且 } 0 < i \leqslant n - t \}|$$

设 $s \leqslant d - t$。于是 C 中重量为 d 的码字构成 t—设计，且 $C^{\perp}$ 中 $B_i \neq 0$ 的任何重量为 $i \leqslant n - t$ 的码字都构成 t—设计。

证明 令 T 为 t 个坐标位置的集合。设 C^T 为 C 去掉这 t 个坐标后所得到的码。由定理 2.5.5 可知，C 中任何 $n - d + 1$ 个列都包含 k 个线性无关的列。又因 $t < d$，故 $n - t \geqslant n - d + 1$，因此 C^T 为 $(n - t, k)$ 码。显然 C^T 的最小重量$\geqslant d - t$。现在考虑 $C^{\perp}$ 的子码 D，其中 D 在 T 上为零。由于 $t < d$，故由推论 2.5.4.1 可知，T 中的 t 个列是 $C^{\perp}$中的线性无关列，因而 D 为 $(n, n - k - t)$ 码。命 $(C^{\perp})^{0T}$ 表示由 D 去掉 T 中的 t 个坐标后所得到的码，于是，$(C^{\perp})^{0T}$ 为 $(n - t, n - k - t)$ 码。显然 C^T 与 $(C^{\perp})^{0T}$ 彼此正交，并且

$$\dim C^T + \dim (C^T)^{0T} = n - t$$

因此

$$(C^{\perp})^{0T} = (C^T)^{\perp}$$

设 $\{B_i'\}$ 为码 $(C^{\perp})^{0T}$ 的重量分布，则有 $B_i' \leqslant B_i$。命

$$s' \triangleq |\{ i \mid B_i' \neq 0 \text{ 且 } 0 < i \leqslant n - t \}|$$

显然有 $s' \leqslant s$。由于 $s \leqslant d - t$，故 $s' \leqslant d - t$。因此 C^T 的最小重量$\geqslant d - t \geqslant s'$。对于码 C^T 和 $(C^T)^{\perp} = (C^{\perp})^{0T}$，上述条件完全适用于定理 7.3.3，从而我们可以得到关于它们的重量分布的普列斯幂矩的唯一解。这个解只依赖于两个码的维数 k 和 $n - k - t$，而与坐标集合 T 的选择无关。

考虑 C 中具有下述性质的重量为 d 的向量，它们在某个固定的势为 t 的坐标集合 T 上为 1。任意一个这样的向量都对应一个

C^T中重量为$d-t$的向量。例如，$t=2$，$T=\{0, 1\}$，则（1 1 0 1 0 0 0）$\in C$对应（0 1 0 0 0）$\in C^T$。反之，由于d是C中的最小重量，故C^T中任意重量为$d-t$的向量必来自C中一个重量为d的向量，且该向量在T上为1。因为C^T中重量为$d-t$的向量数目与集合T的选择无关，故C中重量为d的向量构成t—设计。

令C_1，…，C_r为$C^\perp$中重量为W（$W\leqslant n-t$）的向量的补，我们证明这些向量构成t—设计。从而由定理7.4.4可得，$C^\perp$中重量为W的向量构成t—设计。考虑在T上为1的所有C_i的集合σ。显然σ中的向量是$(C^\perp)^{0T}$中重量为W的向量的补。由于$(C^\perp)^{0T}$的重量分布与T的选择无关，故$|\sigma|$是一个常数，与T的选择无关。（证毕）

下面，我们举例说明定理的应用。

例7.5.1 令C为（24，12，8）二元扩展戈莱码，且令$t=5$。因为$C=C^\perp$，故对于$i\leqslant 24-5=19$，当$i=8$，12，16时，$B_i\neq 0$。因此，$s=3$。由于$3\leqslant 8-5=3$，故$C(=C^\perp)$中重量为8、12和16的向量构成5—设计。

注意定理7.5.4只说明C中重量为8、12和16的向量构成5—设计，但并未给出其它参数v、k和λ。

事实上，C中重量为8、12和16的向量分别构成5—(24，8，1)设计（或斯坦纳系统S(5，8，24)），5—(24，12，48）设计和5—(24，16，78）设计。其中，5—(24，16，78）设计是5—(24，8，1）设计的补设计。

此外，根据推论7.4.3，由于S(5，8，24）的存在，可以推导出S(4，7，23)、S(3，6，22）和S(2，5，21）也存在。

例7.5.2 设C'为二元（23，12，7）戈莱码。因为C'是完备码，故我们知道（推论7.5.2.2）C'中重量为7的码字构成4—(23，7，1）设计。

设$\{B_i\}$为$(C')^\perp$的重量分布。由于$(C')^\perp$是二元（23，11，

8）自正交码，故除非 $i=8$、12或16，皆有 $B_i=0$。若取 $t=4$，则 $n-t=19$，且 $s=3$。因为 $3=d-t=7-4$，故 $(C')^{\perp}$ 中重量为8、12和16的向量都包含4—设计。由于 $(C')^{\perp}\subseteq C'$，故 C' 中重量为8、12和16的向量也包含4—设计。此外，C' 中重量为11和15的向量亦构成4—设计。

研究设计与码之间的联系具有重要意义。一方面，利用码的性质可以构造出新的设计；另一方面，利用码中形成的设计，可以建立译码方案，或获取有关码的其它信息等等。

第八章　代数几何码

§8.1 历史背景

代数几何码理论的确应归功于前苏联数学家高帕。他在70年代末及80年代初所发表的一系列重要论文，将代数几何的理论与方法系统地应用于编码理论中。发现代数几何中的许多概念与结论均可转换成纠错编码的相应性质，使得原来线性码中的重要参数，诸如码长、距离、维数等，具有全新的几何意义及算术意义。继此之后，许多著名编码学家诸如拉卓德（Lachaud），林特（Van Lint），斯普林格（Springer）及茨伐斯曼等人，在这一领域中做了许多重要的工作。特别是茨伐斯曼等人的工作，基于代数几何与高帕码的思想，利用模曲线构造了优于基尔伯特-瓦尔莎莫夫界的码序列。这是多年来关于基尔伯特-瓦沙莫夫限在理论上的重大突破，在编码学界产生了轰动。

由于上述的一系列奠基性的工作，使代数几何码形成了编码理论中具有指导性的重要研究领域。尽管代数几何码走向实用阶段尚有一段艰难的历程，但是许多编码学家都预言这可能是本世纪最后10年的事情。

代数几何作为现代数学的重要研究领域在我国仍属初级阶段，特别是这一学科目前尚不为我国广大编码学者所熟悉。考虑到本书的对象，我们只能对代数几何码的基本概念及重要结论作一个浅显的介绍，不追求理论的严谨与系统，许多重要结果仅以实例说明。有志于深入研究这一领域的读者请查阅有关文献及专著。

§8.2 代数几何的研究对象

代数几何是几何学中的一个重要研究领域。它研究平面代数曲线，空间代数曲线和代数曲面，一般地研究 n 维空间的代数簇。所谓代数簇，就是由一组代数方程所确定的点集，以及由这些点集通过一定的规则导出的对象。

例如，在普通直角坐标中，由代数方程

$$F(x, y)=0$$

所决定的曲线即为平面代数曲线。这里 $F(x, y)$ 是关于变量 x，y 的二元多项式。平面上的直线、圆锥曲线都是代数曲线，但是 $y-\sin x=0$ 所决定的正弦曲线便不是代数曲线。类似地，由三元多项式

$$F(x, y, z)=0$$

决定的点集即为代数曲面。两个无关且相容的三元代数方程组

$$F_1(x, y, z)=0$$

$$F_2(x, y, z)=0$$

所决定的点集，即为空间代数曲线。一般地，由 n 元代数方程组

$$F_i(x_1, x_2, \cdots, x_n)=0, \quad i=1, 2, \cdots, m$$

所决定的点集即为代数簇。研究一次曲线（直线）及一次曲面（平面），以及二次曲线和曲面是普通解析几何中的内容。在19世纪以前，代数几何是从研究三次及四次曲线及曲面的分类开始的。从19世纪末开始，人们才开始研究一般代数簇的系统结构。在代数几何的研究中，采用拓扑学及抽象代数方法则是本世纪的事情。

在代数几何码中，主要的工具是定义于有限域上的代数曲线，特别是仿射曲线及射影曲线。因此，以下我们着重介绍与此有关的基本概念。

§8.3 仿射空间与仿射变换

假设 k 是一个域，V_k^n 代表 k 上定义的 n 维向量空间。借助于 V_k^n 可引入一个 n 维仿射空间。

定义8.3.1 一个 n 维仿射空间 A_k^n 是点 P，Q，R，…的集，满足

（1）每一个有序点偶（P，Q），恰有 $\boldsymbol{v}\in V_k^n$ 与之对应，记为 $\boldsymbol{PQ}=\boldsymbol{v}$。

（2）每一个点 $P\in A_k^n$ 及每一向量 $\boldsymbol{v}\in V_k^n$ 恰有一点 $Q\in A_k^n$ 使 $\boldsymbol{PQ}=\boldsymbol{v}$。

（3）对于 A_k^n 中任意三点 P，Q，R，恒有

$$\boldsymbol{PQ}+\boldsymbol{QR}=\boldsymbol{PR}$$

设 $\boldsymbol{v}\in V_k^n$。由定义 8.3.1 之（2），对于每一点 $P\in A_k^n$，恰有一点 $Q\in A_k^n$ 使 $\boldsymbol{PQ}=\boldsymbol{v}$。由此定义了 A_k^n 上的一个映射

$$T_v: P\longrightarrow Q,\quad PT_v=Q$$

称此映射 T_v 为 A_k^n 上的一个平移（见图 8-1）。

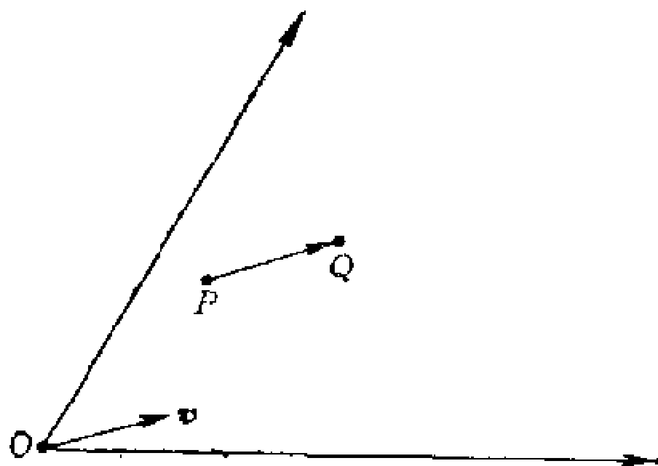

图 8-1

在 A_k^n 中任选一点 O，称为原点。于是由定义 8.1.1，对于每一个 $P\in A_k^n$，存在 $\boldsymbol{v}\in A_k^n$ 使 $\boldsymbol{OP}=\boldsymbol{v}$，称 $\boldsymbol{v}$ 为点 P 的位置向量。若 $\boldsymbol{v}$ 在 V_k^n 的一个基底 $\boldsymbol{e}_1$，$\boldsymbol{e}_2$，…，$\boldsymbol{e}_n$ 之下的坐标为（x_1，x_2，…，x_n），则称点 P 具有坐标为（x_1，x_2，…，x_n）。特别，点

O之坐标为（0，0，…，0）。A_k^n的仿射坐标系记为$\{O, e_1, e_2, \cdots, e_n\}$。

仿射坐标是比普通直角坐标更为一般的坐标系。

A_k^n中点的平移变换可通过V_k^n中的（位置）向量的平移表达。

事实上，从A_k^n中的点P与V_k^n中位置向量$\boldsymbol{OP}=\boldsymbol{v}$之间的一一对应关系，平移变换$PT_b=Q$（$\boldsymbol{b}\in V_k^n$），即$\boldsymbol{PQ}=\boldsymbol{b}$，可视为向量$\boldsymbol{OP}$在变换$T_b$之下变换为向量$\boldsymbol{OQ}$，记为$\boldsymbol{OP}T_b=\boldsymbol{OQ}$。由于$\boldsymbol{OP}=\boldsymbol{v}$，$\boldsymbol{OQ}=\boldsymbol{OP}+\boldsymbol{PQ}=\boldsymbol{v}+\boldsymbol{b}$，因此（见图8-2）

$$\boldsymbol{v}T_b=\boldsymbol{V}+\boldsymbol{b}$$

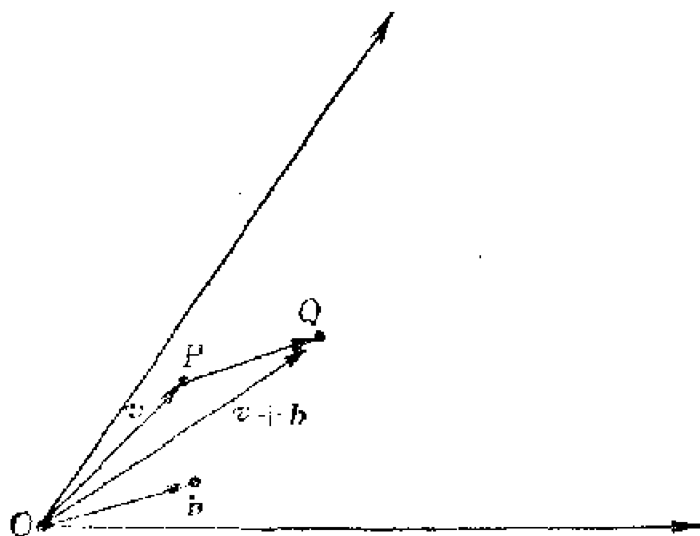

图 8-2

进一步，我们还可以建立仿射子空间的概念。

定义8.3.2 设α^m为n维仿射空间A_k^n的非空子集，S^m为V_k^n的m维向量子空间。如果在A_k^n与V_k^n的相应关系下，α^m恰好是相应于S^m的一个仿射空间，则称α^m是A_k^n的一个m维仿射子空间。

A_k^n的一维仿射子空间α^1称为直线，二维仿射子空间α^2称为平面。

依据仿射坐标，我们可以把仿射空间中的几何图象建立相应的方程。

例如，考虑A_k^2中一条直线，它通过点$P=(p_1, p_2)$，且该

直线（作为一维仿射空间）相应的一维向量子空间以 $\boldsymbol{v}=(v_1, v_2)$ 为基底（见图 8-3）。设 $X=(x_1, x_2)$ 为该直线上任意一点。于是 $\boldsymbol{PX}$ 必为该直线相应的一维向量子空间中的向量，因而可写成 $\boldsymbol{PX}=\rho V(\rho\in k)$。又因 $\boldsymbol{PX}=\boldsymbol{OX}-\boldsymbol{OP}=(x_1, x_2)-(p_1, p_2)=(x_1-p_1, x_2-p_2)$，$\rho\boldsymbol{v}=(\rho v_1, \rho v_2)$，故

$$(x_1-p_1, x_2-p_2)=(\rho v_1, \rho v_2)$$

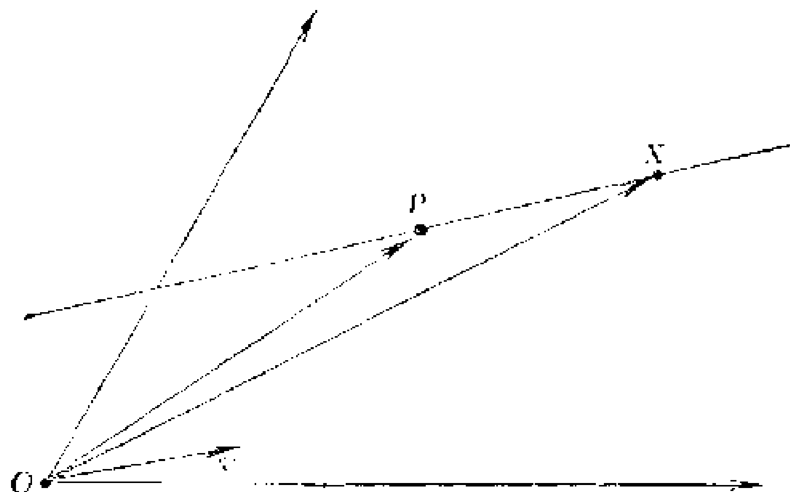

图 8-3

由于 $V\neq 0$（基向量），不妨设 $v_1\neq 0$。于是由 $x_1-p_1=\rho v_1$ 得

$$\rho=\frac{x_1-p_1}{v_1}$$

将 ρ 代入到 $x_2-p_2=\rho v_2$ 中，便有

$$v_2x_1-v_1x_2+(v_1p_2-v_2p_1)=0$$

令 $a_1=v_2$，$a_2=-v_1$，$a_0=v_1p_2-v_2p_1$，便有

$$a_1x_1+a_2x_2+a_0=0 \tag{8-1}$$

其中 a_1，a_2 不全为 0。

反过来，每一个形如式（8-1）的一次方程均代表 A_k^2 中的一条直线。事实上，考虑满足方程（8-1）的所有点 $X=(x_1, x_2)$。由于 a_1，a_2 不全为零，不妨设 $a_1\neq 0$。于是 $x_1=-a_1^{-1}(a_0+a_2x_2)$。选取 $P=(-a_1^{-1}a_0, 0)$，$\boldsymbol{v}=(-a_2, a_1)\neq 0$，使有

$$\boldsymbol{X}=(-a_1^{-1}a_0, 0)+\rho(-a_2, a_1)=\boldsymbol{P}+\rho V,$$

$$\rho=a_1^{-1}x_2$$

此处点 $\boldsymbol{X}$ 与点 $\boldsymbol{P}$ 为点X与P的位置向量。这表明方程（8-1）代表通过点P且由向量 $\boldsymbol{v}$ 构成的直线。

类似于上述方法，我们可以建立仿射空间中的高次曲线的方程。仿射空间中的曲线称为**仿射曲线**。

在本节之末，我们引入仿射变换的概念。

设 $\boldsymbol{e}_1$，$\boldsymbol{e}_2$，…，$\boldsymbol{e}_n$ 为 n 维向量空间 V_k^n 的基底。设$\{O$，e_1，e_2，…，$e_n\}$为相应的 n 维仿射空间 A_k^n 的坐标系。设$X=(x_1, x_2, \cdots, x_n)$ 为 A_k^n 中任意一点。所谓**仿射变换**是指线性变换

$$Y=CX+\boldsymbol{b} \tag{8-2}$$

其中

$$C=\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix}$$

为域 k 上的非异矩阵，$\boldsymbol{b}=(b_1, \cdots, b_n)$ 为 A_k^n 中一点。因此，仿射变换即为 A_k^n 上的非异齐次线性变换再加上平移。在变换（8-2）之下，点$X=(x_1, \cdots, x_n)$ 变为点$Y=(y_1, \cdots, y_n)$。

仿射几何就是研究在仿射变换之下，几何图形的不变性质及不变量。例如，在仿射变换下，直线仍变成直线。因此，直线是仿射几何的研究对象。但是，在 A_k^2 中椭圆 $b^2x_1^2+a^2x_2^2-a^2b^2=0$ 经过仿射变换 $x_1=r^{-1}ax_1'$，$x_2=r^{-1}bx_2'$ 可变为圆：$x_1'^2+x_2'^2-r^2=0$。因此，在仿射几何中，圆与椭圆是一回事（仿射等价）。

§8.4 射影空间与射影变换

引入 n 维仿射空间的出发点是 n 维向量空间。引入 n 维射影空间的出发点则是域 k 上的 $n+1$ 维向量空间 V_k^{n+1}。

设 $\boldsymbol{V}$，$\boldsymbol{W}\in V_k^{n+1}$。若存在 $r\neq 0$（$r\in k$）使$\boldsymbol{W}=r\boldsymbol{V}$，则称**向量$V$与$W$等价**。

在等价的意义下，V_k^{n+1} 中的全部向量被分成等价类。零向量 $\boldsymbol{0}$ 构成由自身代表的一类。记为$[\boldsymbol{0}]$。如果一个类中包含向量V，

则此类用$[V]$代表。

定义8.4.1 在V_k^{n+1}中所建立的每一个异于$[0]$的类称为射影点。所有射影点的全体所成之集称为域k上的n维射影空间，记作P_k^n。

因此，P_k^n中的点是V_k^{n+1}中的一维子空间。V_k^{n+1}中的二维子空间称为P_k^n中的射影直线，三维子空间称为P_k^n中的射影平面，V_k^{n+1}的m（$m>3$）维子空间称为P_k^n中的（$m-1$）维超平面。

在射影空间中可以引进齐次坐标的概念。

设e_1，…，e_n，e_{n+1}是V_k^{n+1}的一个基底。于是P_k^n中每一点$[X]$皆可表为

$$[X]=(x_1e_1+\cdots x_ne_n+x_{n+1}e_{n+1})=\left[\sum_{j=1}^{n+1}x_je_j\right]$$

称（x_1，…x_n，x_{n+1}）为点$[X]$的射影齐次坐标。

显然，若（x_1，…，x_n，x_{n+1}）为点$[X]$的齐次坐标，则对于任意$r\in k$，$r\neq0$，（rx_1，…，rx_n，rx_{n+1}）亦为点$[X]$的齐次坐标。因为$[X]=[rX]$，所以，在射影空间中的点由坐标比$x_1:\cdots:x_n:x_{n+1}$决定。反之，每一个比值$x_1:\cdots:x_n:x_{n+1}$（$x_1,\cdots,x_n$，x_{n+1}不全为0）决定P_k^n中唯一的一点。点$[X]$的齐次坐标有时也表为（$x_1:\cdots:x_n:x_{n+1}$）。

作为例子，我们建立射影平面P_k^2中直线的齐次坐标方程。

设$[Y]=(y_1,\ y_2,\ y_3)$，$[Z]=(z_1,\ z_2,\ z_3)$为该直线上两点，$[X]=(x_1,\ x_2,\ x_3)$为该直线上任意一点。这表明相应的V_k^3中向量X，Y，Z线性相关，即存在不全为0的λ_1，λ_2，λ_3使$\lambda_1X+\lambda_2Y+\lambda_3Z=0$，即齐次方程组

$$\lambda_1x_1+\lambda_2y_1+\lambda_3z_1=0$$

$$\lambda_1x_2+\lambda_2y_2+\lambda_3z_2=0$$

$$\lambda_1x_3+\lambda_2y_3+\lambda_3z_3=0$$

有非零解（λ_1，λ_2，λ_3）。而这只有在

$$\begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix} = 0 \tag{8-3}$$

时才成立。而式（8-3）可写成

$$u_1x_1+u_2x_2+u_3x_3=0 \tag{8-4}$$

其中

$u_1=y_2z_3-y_3z_2$，$u_2=y_3z_1-y_1z_3$，$u_3=y_1z_2-y_2z_1$ 并且 u_1, u_2, u_3 不全为 0（否则$\mathbf{Y}$与$\mathbf{Z}$将线性相关）。

另一方面，若点$[\mathbf{X}]$不在该直线上，则$\mathbf{X}$，$\mathbf{Y}$，$\mathbf{Z}$必线性独立，因而式（8-3）必不为 0，即$[\mathbf{X}]$之坐标不满足式（8-4）。

式（8-4）即为P_k^2中射影直线之一般方程。类似地，我们可建立射影空间中高次曲线的方程。射影空间中的曲线称为射影曲线。

我们现在讨论射影空间与仿射空间之间的关系。

假设用以决定射影空间P_k^n中点坐标的基底为$\{e_1, \cdots, e_n, e_{n+1}\}$（张成$V_k^{n+1}$），而产生仿射空间$A_k^n$之基底为$\{e_1, e_2, \cdots, e_n\}$。现将$P_k^n$中的点分为两类：第一类，$x_{n+1}\neq 0$；第二类，$x_{n+1}=0$。对于第一类的点可写为

$$(x_1, \cdots, x_n, x_{n+1})=(x_1/x_{n+1}, \cdots, x_n/x_{n+1}, 1)$$

于是在P_k^n中的第一类点与A_k^n中的点之间可建立如下的一一对应关系：

$$(y_1, \cdots, y_n, 1)\in P_k^n \longleftrightarrow (y_1, \cdots, y_n)\in A_k^n$$

在A_k^n中没有一个点对应于P_k^n中的第二类点。

由于射影空间P_k^n中的第一类点包含了所有对应于仿设空间A_k^n中的点，同时在射影空间中还有第二种点。因此射影空间P_k^n可视为由仿射空间A_k^n中的点添加第二种点，即所谓虚点而获得的模型。由于所有虚点均对应于$x_{n+1}=0$的射影点，因此这种射影点位于一个射影超平面上，并且全部这种点对应于仿射空间A_k^n的镜像是（$n-1$）维线性子空间，即所谓（$n-1$）维流型。在A_k^2中是直线，在A_k^3中是平面，等等。在射影空间中，上

述的虚点也称为**无穷远点**。

在仿射几何中有两条直线平行的概念，而在相应的射影几何中任何两条直线均相交于唯一的一点。事实上，设仿射平面A_k^2中直线l的方程为

$a_1x_1+a_2x_2+a_3=0$，（a_1，a_2不全为0），则所有A_k^2中与l平行的直线方程均可写成上述形式，其中a_1，a_2固定，a_3任意变化。将坐标齐次化，便得到相应的射影平面P_k^2中对应的直线方程

$$a_1\frac{x_1}{x_3}+a_2\frac{x_2}{x_3}+a_3=0\text{ 或 }a_1x_1+a_2x_2+a_3x_3=0$$

显然，位于该直线上具有$x_3=0$的点只有一个，其齐次坐标为（a_2，$-a_1$，0）。由于（a_2，$-a_1$，0）中不出现a_3，故所有与已知直线l平行的直线均含有该点。因此在射影平面的仿射模型中，所有平行的直线均相交于唯一的虚点，并且每一个虚点均为一直线以及与其平行的所有直线的交点。因此在射影平面上，每两条直线均相交于唯一的一点（实点或虚点）。

同样，在射影空间P_k^3中，所有平行的平面均相交于唯一的一条虚直线，并且每条虚直线是一个平行平面簇的交线。

综上所述，P_k^1的模型是由A_k^1添加一个虚点构成。P_k^2的模型是由A_k^2添加一条虚直线（其上的点均为虚点）而成。P_k^3的模型是由A_k^3添加一个所谓虚平面（其上的点均为虚点）而成。一般地，P_k^n的模型是由A_k^n添加一个（$n-1$）维虚超平面（其上的点均为虚点）而成。

最后介绍射影变换的概念。

设$\boldsymbol{x}=(x_1,\ \cdots,\ x_n,\ x_{n+1})$与$r\boldsymbol{x}=(rx_1,\ \cdots,\ rx_n,\ rx_{n+1})$（$r\neq0$）为向量空间$V_k^{n+1}$中两个彼此等价的向量。设$L_A$为$V_k^{n+1}$的一个非异线性变换，该变换的矩阵为$(n+1)\times(n+1)$非异矩阵$A$。于是

$$(r\boldsymbol{x})L_A=(r\boldsymbol{x})A=r(\boldsymbol{x}A)=r(\boldsymbol{x}L_A)=\boldsymbol{x}(rA)=\boldsymbol{x}L_{rA}$$

其中L_{rA}是V_k^{n+1}上以非异矩阵rA为变换矩阵的线性变换。由此可见，如果我们把成比例的两个非异矩阵A与rA（$r\neq0$）视

为等价。相应地，把两个非异线性变换 L_A 与 L_{rA}视为等价，则上式表明：V_k^{n+1} 中等价的线性变换把 V_k^{n+1} 中等价的向量变为等价向量。如所周知，在 V_k^{n+1} 中的非异线性变换把m维子空间仍变成m维子空间。特别，这一变换把一维子空间仍变为一维子空间。这就导致了射影空间 P_k^n 中点的变换。

上述讨论指出，V_k^{n+1} 中非异线性变换等价类把 P_k^n 中的点仍变成 P_k^n 中的点，这种对应还是一一对应。

称 V_k^{n+1} 中非异线性变换等价类为射影空间 P_k^n 的一个**射影变换**。

在 P_k^n 中，射影变换的齐次坐标表达式可写成

$$(\rho x'_1,\ \cdots,\ \rho x'_n,\ \rho x'_{n+1})=(x_1,\ \cdots,\ x_n,\ x_{n+1})\cdot\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} & a_{1n+1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & a_{nn+1} \\ \\ a_{n+11} & a_{n+12} & \cdots & a_{n+1n} & a_{n+1n+1} \end{bmatrix}$$

其中A为相应射影变换的矩阵。

研究在射影变换下不变的图形性质与不变量，是射影几何学的课题。射影几何学有丰富的研究内容。

§8.5　在有限域上的仿射曲线与射影曲线

设 F_q 代表q阶有限域（有时也记作$GF(q)$）。又设 $\overline{F}_q$ 代表 F_q 的代数闭包，即包含 F_q 的最小代数闭域。可以证明

$$\overline{F}_q=\bigcup_{m=1}^{\infty}F_{q^m}$$

今后将以 $\overline{F}_q$ 代替前几节讨论的任意域k，并且考虑点的坐标取在 $\overline{F}_q$ 上的仿射平面与射影平面，分别用 $A^2(\overline{F}_q)$ 及 $P^2(\overline{F}_q)$ 代表。

设$F(x, y)$ 代表 $\overline{F}_q$ 上的二元多项式，它在 $\overline{F}_q$ 上的全部根便定义为仿射平面 $A^2(\overline{F}_q)$ 上的一条**仿射曲线**。多项式$F(x, y)$ 的次数称为该**曲线的阶**。

定义8.5.1 在仿射平面上 $A^2(\overline{F}_q)$ 的点（a，b），若 a，$b\in F_q$，则称点（a，b）为 $A^2(\overline{F}_q)$ 上的**有理点**。

对于 m 次二元多项式 $F(x, y)$，它定义了一条 m 阶仿射曲线，记为 C。经过齐次化，$z^m F(x/z, y/z)$ 便得到一个三元 m 次齐次多项式，记为 $F(x, y, z)$。

例如，考虑 3 次二元多项式

$$F(x, y)=y^2-x^2(x+1)$$

它定义了仿射平面上一条 3 阶仿射曲线。经过齐次化

$$z^3F(x/z, y/z)=F(x, y, z)=y^2z-x^3-x^2z$$

齐次化的过程相当于引进齐次坐标。

一般由 m 次二元多项式 $F(x, y)$ 经过齐次化得到的三元 m 次齐次多项式 $F(x, y, z)$ 便定义了射影平面上的一条 m 阶代数曲线，称为**m阶射影曲线**。它是由仿射曲线 C 上的点添加某些无穷远点所构成的射影平面上的 m 阶代数曲线。

反过来，每一条 m 阶射影曲线 $F(x,y,z)=0$ 也可通过非齐次化方法化为 m 阶仿射曲线 $F(x, y, 1)=0$。例如 5 阶射影曲线

$$F(x, y, z)=x^5+y^5-z^5=0$$

可化为

$$F(x, y)=x^5+y^5-1=0$$

这相当于由原来的 m 阶射影曲线去掉某些无穷远点所产生的 m 阶仿射曲线。

定义8.5.2 在射影平面 $P^2(\overline{F}_q)$ 上的点（a，b，c），当 $c\neq 0$ 时，a/c，$b/c\in F_q$；当 $c=0$ 时（此时 a，b 中至少有一不为 0），$a/b\in F_q$（$b\neq 0$）或 $b/a\in F_q$（$a\neq 0$）。则称点（a，b，c）为 $P^2(\overline{F}_q)$ 上的**有理点**。

曲线上这些有理点有时可枚举出来。

例8.1 在 $P^2(\overline{F}_4)$ 上找出曲线

$$y^2z+yz^2=x^3+x^2z+xz^2+z^3 \tag{8-5}$$

上的全部有理点。

熟知$F_4=\{0, 1, \alpha, \beta\}$，$\beta=\alpha+1=\alpha^2$。经过计算，该曲线上的全部有理点共有9个，见表8-1。

表 8-1

	Q	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
x	0	0	0	1	1	α	α	β	β
y	1	α	β	0	1	α	β	α	β
z	0	1	1	1	1	1	1	1	1

点Q（0，1，0）是无穷远点。曲线（8-5）是亏格为1的代数曲线，称为椭圆曲线。椭圆曲线是编码理论中要讨论的重要曲线，以后我们会进一步解释。

在实践上，真正算出给定曲线的全部有理点，或退一步，算出这些有理点的个数，均是相当困难的工作。

如果多项式$F(x, y)$在F_q的任何扩域F_{q^m}上均无异于常数的因式，则称相应的曲线为**不可约曲线**。判断一条曲线的不可约性，也是一件相当困难的事情。

§8.6 RS码与高帕(Goppa)码

为了讨论一般的代数几何码，我们首先来回顾一下经典的RS码及高帕码。

我们知道，RS码是F_q（$q\neq 2$）上码长为$n=q-1$的本原BCH码，该码的生成多项式为

$$g(x)=\prod_{i=1}^{d-1}(x-\alpha^i)$$

其α为F_q的本原域元素。RS码是码长为n（$=q-1$）、信息位数为$n-d+1$，最小距离为d的极大最小距离可分码(n，$n-d+1$，d)，亦即MDS码。

像所有线性码一样，对于RS码（n，$n-d+1$，d）增加一个全监督位后，便成为扩展RS码，其码长为$n+1$（$=q$），

信息位数仍为 $n-d+1$ 的（$n+1$，$n-d+1$）码。如所周知，这个码的最小距离为 $d+1$，因而扩展 RS 码仍为 MDS 码。

我们现在遵循里德(Reed)与所罗门(Solomon)原来的编码方法，从另一角度来建立扩展 RS 码。

为了方便，我们取 $n=q$，F_q 中的元素记成

$$a_i=\alpha^i,\ (0\leqslant i\leqslant q-2),\ a_{q-1}=0$$

其中 α 为 F_q 的本原域元素。令

$$L=\{f\in F_q[x]\mid \deg f\leqslant k-1\},\quad k<n$$

我们定义一个码 C 为

$$C=\{(f(a_0),\ f(a_1),\ \cdots,\ f(a_{q-1}))\mid f\in L\}$$

码 C 显然是线性的，码长 $n=q$，信息位数为 k，即 L（作为线性空间）的维数。又因 L 中的多项式次数 $\leqslant k-1$，故不可能多于 $k-1$ 个零点，从而码 C 的最小距离 $d_m\geqslant n-k+1$。另一方面，因任何线性码的最小距离至多为该码的监督位数加 1（辛格里通限），即

$$d_m\leqslant n-k+1$$

因此，$d_m=n-k+1$。这表明码 C 是（n，k，$n-k+1$）线性码，亦即 MDS 码。

不难看出，码 C 等价于扩展 RS 码，事实上，设 $f(x)=\sum_{j=0}^{k-1}a_jx^j$，且令 $c_i=f(a_i)$，$0\leqslant i\leqslant q-2$。于是，如果 $1\leqslant l\leqslant q-k-1$，则

$$\sum_{i=0}^{q-2}c_i(\alpha^l)^i=\sum_{i=0}^{q-2}(\alpha^l)^i\sum_{j=0}^{k-1}a_j(\alpha^i)^j=\sum_{j=0}^{k-1}a_j\sum_{i=0}^{q-2}(\alpha^{l+j})^i$$

注意到

$$x^{q-1}-1=(x-1)\sum_{i=0}^{q-2}x^i$$

从而在 F_q 中每一元素 $a\neq 0,1$，均满足 $\sum_{i=0}^{q-2}a^i=0$。由于

$1 \leqslant l + j \leqslant q - k - 1 + k - 1 = q - 2$，故 $\sum_{i=0}^{q-2} (\alpha^{l+j})^i = 0$。

因此

$$\sum_{i=0}^{q-2} c_i (\alpha^l)^i = 0$$

这表明 $C = (c_0, c_1, \cdots, c_{q-2})$ 是最小距离为 $q - k$ 的 RS 码中的码字。将此码再添加一个全监督位，即为扩展 RS 码。RS码在磁盘纠错技术中很有用处。

为了进一步讨论代数几何码，我们将 RS 码的第二种定义再加以推广。

设 $\xi_i (\neq 0) \in F_q$ $(i = 1, \cdots, n)$，$\{\alpha_1, \cdots, \alpha_n\} \subset \{1, \alpha, \cdots, \alpha^{q-2}\}$，且 $\alpha_1, \cdots, \alpha_n$ 彼此不同。于是可定义一个码字为

$$C = \{(\xi_1 f(\alpha_1), \cdots, \xi_n f(\alpha_n)) | f \in L\}$$

这个码的构成相当于如下的线性映射：

$$\begin{array}{ccc} L & \longrightarrow & (F_q)^n \\ \Psi & & \Psi \\ f & \longrightarrow & (\xi_1 f(\alpha_1), \cdots, \xi_n f(\alpha_n)) \end{array}$$

显然 C 仍为最小距离 $n - k + 1$ 的线性码 $(n, k, n - k + 1)$，即为 MDS 码。

为增大码长，上面所构成的线性码还可在 F_q 的扩域 F_{q^m} 上考虑。设

$$L = \{f \in F_{q^m}[x] | \deg f \leqslant k - 1\}, \quad k < n,$$

再设 $\xi_i (\neq 0) \in F_{q^m} (i = 1, 2, \cdots, n)$，$\xi = (\xi_1, \cdots, \xi_n)$，并且取 F_{q^m} 中 n 个不同元素 $\alpha_1, \cdots, \alpha_n$，置 $\alpha = (\alpha_1, \cdots, \alpha_n)$，于是可构造一个线性码

$$C = \{(\xi_1 f(\alpha_1), \cdots, \xi_n f(\alpha_n)) | f \in L\}$$

码 C 仍为 $(n, k, n - k + 1)$ 线性码，即为 MDS 码。称该码为广义 RS 码，记为 $GRS_k(\alpha, \xi)$。

现在我们再来讨论高帕码。

设 F_q 为基域，$g(z)\in F_{q^m}[z]$，$L=\{\alpha_1, \cdots, \alpha_n\}$，$\alpha_i\in F_{q^m}(i=1, \cdots, n)$，$\alpha_i\neq\alpha_j\ (i\neq j)$。设 $g(z)$ 的根不在 L 中，即 $g(\alpha_i)\neq 0\ (i=1, \cdots, n)$。于是定义

$$C=\left\{(c_1, \cdots, c_n)\in(F_q)^n \left| \sum_{i=1}^{n}\frac{c_i}{z-\alpha_i}\equiv 0 \bmod g(z)\right.\right\}$$

C 即为经典的高帕码，记为 $\Gamma(L, g)$，其中 $g(z)$ 称为高帕多项式。

为使导入代数曲线上定义的线性码更为自然，我们将高帕码的定义进一步推广。

假设 $f(z)=\phi(z)/\psi(z)$ 是 F_{q^m} 上的有理函数，即 $\phi(z), \psi(z)\in F_{q^m}[z]$。现在考虑 F_{q^m} 上所有具备下列性质的有理函数全体：

（1）$f(z)$ 以 $g(z)$ 的所有零点为零点（$g(z)$ 即为前述定义中的 F_{q^m} 上的高帕多项式)，且 $f(z)$ 在这些零点上的级至少为 $g(z)$ 在这些零点上相应的级。

（2）$f(z)$ 除了在 $L=\{\alpha_1, \cdots\alpha_n\}$ 中的某些点上可能具有一级极点外别无其它极点。

这里 $f(z)$ 的极点、极点的级，以及下面提到的 $f(z)$ 在极点 α_i 上的留数 $\text{Res}_{\alpha_i} f$ 与普通复函数论中的定义类似，此处不再重复。

当 $f(z)$ 取遍具有上述性质（1），（2）的全部 F_{q^m} 上的有理函数时（注意，这些有理函数的全体构成一个线性空间），在 F_{q^m} 上便可定义一个线性码，它由形如

$$(\text{Res}_{\alpha_1} f, \cdots, \text{Res}_{\alpha_n} f)$$

的 n 重构成。

因为高帕码是定义在 F_q 上的线性码，显然，高帕码是上述定义的码的子域（$F_q\subset F_{q^m}$）子码。在高帕码中

$$R_c(z)=\sum_{i=1}^{n}\frac{c_i}{z-\alpha_i}$$

即为 F_q 上的有理函数，它满足条件（1），（2），并且

$c_i = \mathrm{Res}_{\alpha_i} R_c(z)$， $i=1, 2, \cdots, n$

为了讨论高帕码与广义 RS 码之间的关系，我们首先需找出高帕码 $\Gamma(L, g)$ 的一致校验矩阵。设 $g(z)=\sum_{i=0}^{t} g_i z^i$，于是

$$\phi(z)=\frac{g(z)-g(x)}{z-x}=\sum_{0\leqslant l+j\leqslant t-1} g_{l+j+1} x^j z^l$$

是关于变量 z 的一个次数 $< t$ 的多项式（对于任何 x）。由于

$$\frac{1}{z-\alpha_i}\equiv\frac{-1}{g(\alpha_i)}\left[\frac{g(z)-g(\alpha_i)}{z-\alpha_i}\right]\mathrm{mod}\ g(z)$$

从而依据 $(z-x)\ \phi(z)=g(z)-g(x)\equiv -g(x)\mathrm{mod}\ g(z)$ 再令 $\xi_i=1/g(\alpha_i)$，关系式

$$\sum_{i=1}^{n}\frac{c_i}{z-\alpha_i}\equiv 0 \quad \mathrm{mod}\ g(z)$$

可改写成

$$\sum_{i=1}^{n} c_i\xi_i \sum_{0\leqslant l+j\leqslant t-1} g_{l+j+1}(\alpha_i)^j z^l = 0$$

对于 $0\leqslant l\leqslant t-1$，上式中 z^l 的系数均为 0。我们看出，$C=(c_1, \cdots, c_n)$ 必与下列矩阵之每一行向量内积为 0：

$$\begin{bmatrix} \xi_1 g_t & \cdots & \xi_n g_t \\ \xi_1(g_{t-1}+g_t\alpha_1) & \cdots & \xi_n(g_{t-1}+g_t\alpha_n) \\ \vdots & \cdots & \vdots \\ \xi_1(g_1+g_2\alpha_1+\cdots+g_t\alpha_1^{t-1}) & \cdots & \xi_n(g_1+g_2\alpha_n+\cdots+g_t\alpha_n^{t-1}) \end{bmatrix}$$

其中第 1 行对应于上述和式中 z^{t-1} 之系数，第 2 行对应于 z^{t-2} 的系数，等等。最后第 t 行对应 z^0 的系数。

如所周知，对上述矩形做初等行变换并不影响 C 与该矩阵行的正交性。由此便得到高帕码 $\Gamma(L, g)$ 的一致校验矩阵为

$$H=\begin{bmatrix} \xi_1 & \xi_2 & \cdots & \xi_n \\ \xi_1\alpha_1 & \xi_2\alpha_2 & \cdots & \xi_n\alpha_n \\ \vdots & \vdots & \cdots & \vdots \\ \xi_1\alpha_1^{t-1} & \xi_2\alpha_2^{t-1} & \cdots & \xi_n\alpha_n^{t-1} \end{bmatrix}$$

现在我们再回过来讨论广义 RS 码 $GRS_k(\alpha, \xi)$，亦即

$$C=\{(\xi_1 f(\alpha_1), \cdots, \xi_n f(\alpha_n)) \mid f\in L\}$$

的生成矩阵。在 $GRS_k(\alpha, \xi)$ 中取 $k=t$，且设 $f(z)=\sum_{i=0}^{t-1} f_i z^i$。于是 C 中的码字可写成

$$\left(\xi_1\sum_{i=0}^{t-1} f_i\alpha_1^i, \cdots, \xi_n\sum_{i=0}^{t-1} f_i\alpha_n^i\right)$$

$$=(f_0, f_1, \cdots, f_{t-1})\begin{bmatrix} \xi_1 & \xi_2 & \cdots & \xi_n \\ \xi_1\alpha_1 & \xi_2\alpha_2 & \cdots & \xi_n\alpha_n \\ \vdots & \vdots & \cdots & \vdots \\ \xi_1\alpha_1^{t-1} & \xi_2\alpha_2^{t-1} & \cdots & \xi_n\alpha_n^{t-1} \end{bmatrix}$$

这表明高帕码 $\Gamma(L, g)$ 的一致校验矩阵恰为 $GRS_k(\alpha, \xi)$ 的生成矩阵。由此可见，高帕码恰为一个广义 RS 码的对偶码的子域子码。

§8.7 代数几何码的构成

在上一节构造 RS 码及广义 RS 码中所使用的多项式 $f(z)$ 可写成

$$z^\delta+a_{\delta-1}z^{\delta-1}+\cdots+a_1z+a_0 \quad (\delta\leqslant k-1),$$

或引进齐次坐标 $z\to\frac{x}{y}$，上式可改写成

$$\frac{x^\delta+a_{\delta-1}x^{\delta-1}y+\cdots+a_1xy^{\delta-1}+a_0y^\delta}{y^\delta} \tag{8-6}$$

$$(\delta\leqslant k-1)$$

考虑射影直线 $X=P^1(\mathbb{F}_q)$，以下有时简写为 P^1。设 $Q=(1, 0)$ 代表 P^1 上的无穷远点。设 $L((k-1)\cdot Q)$ 代表点 Q 至多

为 $k-1$ 级极点的，形如式（8-6）的有理函数全体。

在 RS 码定义中的 α_1，α_2，…，α_n 对应于 $X=P^1(\overline{F}_q)$ 上的 F_q—有理点 $P_1=(\alpha_1, 1)$，$P_2=(\alpha_2, 1)$，…，$P_n=(\alpha_n, 1)$。在 $X=P^1(\overline{F}_q)$ 上的全部有理点共有 $q+1$ 个：

$(0, 1)$，$(1, 1)$，$(\alpha, 1)$，$(\alpha^2, 1)$，…，$(\alpha^{q-2}, 1)$，$(1, 0)$

因此，RS 码从几何的观点来看，相当于从 $L((k-1)\cdot Q)$ 到 $(F_q)^n$ 的一个映射。在这一映射之下，将 $L((k-1)\cdot\infty)$ 上的每一个于点 $Q=(1, 0)$ 至多为（$k-1$）级极点的，形如式（8-6）的有理函数。取其在 $X=P^1(\overline{F}_q)$ 上 n 个指定点 P_1，…，P_n 的值，便得到 $(F_q)^n$ 中的一个向量（$f(P_1)$，…，$f(P_n)$），即为一个码字。图（8-4）给出了这种码的几何解释。

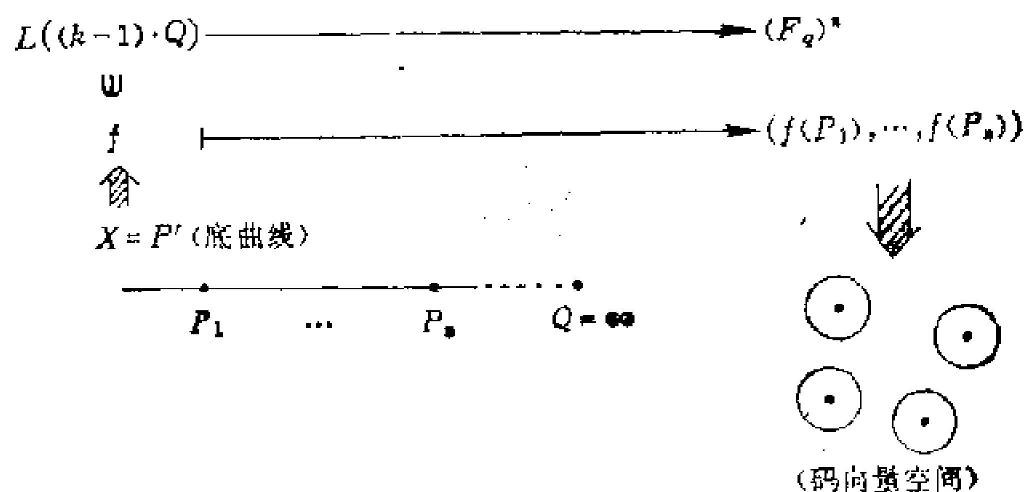

图 8-4

从上述 RS 码的几何解释中，我们看到，这种码是由在射影直线 $X=P^1$ 上的有理函数及有理点 P_1，…，P_n 所确定的。称 $X=P^1$ 为**底曲线**。

激发起构造代数几何码想法的出发点就是将射影直线 $X=P^1$ 由射影平面 P^2 上的代数曲线来取代，并且考虑以这条代数曲线上的指定点 Q_1，…，Q_l 分别至多为 m_1，…，m_l 级极点的全部有理函数，记为 $L(G)$，$G=\sum_{j=1}^{l} m_jQ_j$。在这条曲线上取定

n 个 F_q—有理点 P_1，…，P_n，从而便构造出一个新的线性码

$$C=\{(f(P_1),\ \cdots,\ f(P_n))\mid f\in L(G)\}$$

如图 8-5 所示。在这里，前述代数曲线也称为底曲线。

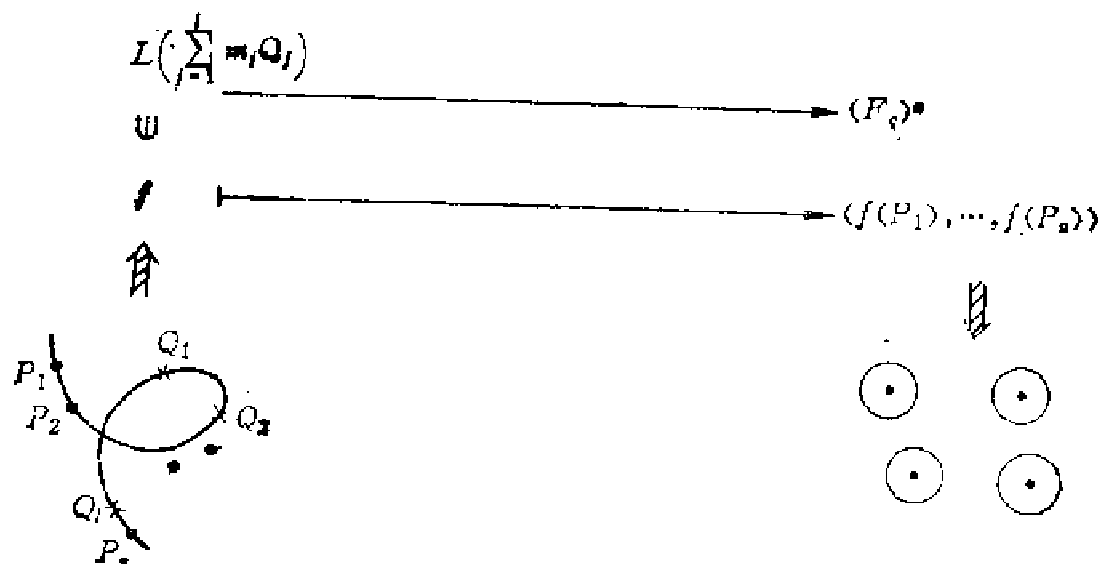

图 8-5

例8.2 考察§8.5 例 8.1中所示椭圆曲线

$$y^2z+yz^2=x^3+x^2z+xz^2+z^3$$

已知该曲线上共有 9 个有理点：Q、P_1，P_2，…，P_8，如表8-1所示。

现令 $G=4Q$，$L(G)=L(4Q)=\{f\mid f$ 为系数，取自 F_4 上且点 Q 至多为其 4 级极点的 X_1 上的有理函数$\}$，其中 X_1 代表椭圆曲线

$$X_1=\{(x,\ y,\ z)\in P^2(\overline{F}_4)\mid y^2z+yz^2=x^3+x^2z+xz^2+z^3\}$$

不难看出，$L(G)$ 为 4 维线性空间，它的一组基底是

$$\psi_1=1,\ \psi_2=x/z,\ \psi_3=y/z,\ \psi_4=x^2/z^2$$

事实上

$$\psi_2=\frac{x}{z}=\frac{x^3}{zx^2}=\frac{y^2z+yz^2+x^2z+xz^2+z^3}{zx^2}$$

$$=\frac{y^2+yz+x^2+xz+z^2}{x^2}$$

因此 ψ_2 以点 $Q=(0,\ 1,\ 0)$ 为2级极点。进一步

$$\psi_4=\left(\frac{x}{z}\right)^2=\frac{x^4+y^2z^2+x^4+x^2z^2+z^4}{z^4}$$

这表明 ψ_4 以点 $Q=(0,\ 1,\ 0)$ 为4级极点。

考虑如下的线性映射 φ_L:

$$\begin{array}{ccc} L(G) & \longrightarrow & (F_4)^8 \\ \Cup & & \Cup \\ f & \longrightarrow & (f(P_1),\ \cdots,\ f(P_8)) \end{array}$$

为了找出所构成的码

$$C=\left\{(f(P_1),\ \cdots,\ f(P_8))\,|\,f=\sum_{i=1}^{4}f_i\psi_i,\ f_i\in F_4\right\}$$

的生成多项式，只需注意

$$\begin{aligned} C&=(f(P_1),\ \cdots,\ f(P_8)) \\ &=\left(\sum_{i=1}^{4}f_i\psi_i(P_1),\ \cdots,\ \sum_{i=1}^{4}f_i\psi_i(P_8)\right) \\ &=(f_1,\ f_2,\ f_3,\ f_4)\begin{bmatrix} \psi_1(P_1) & \psi_1(P_2) & \cdots & \psi_1(P_8) \\ \psi_2(P_1) & \psi_2(P_2) & \cdots & \psi_2(P_8) \\ \psi_3(P_1) & \psi_3(P_2) & \cdots & \psi_3(P_8) \\ \psi_4(P_1) & \psi_4(P_2) & \cdots & \psi_4(P_8) \end{bmatrix} \end{aligned}$$

由此可见码 C 的生成矩阵为

$$\begin{bmatrix} \psi_1(P_1) & \psi_1(P_2)\cdots\psi_1(P_8) \\ \psi_2(P_1) & \psi_2(P_2)\cdots\psi_2(P_8) \\ \psi_3(P_1) & \psi_3(P_2)\cdots\psi_3(P_8) \\ \psi_4(P_1) & \psi_4(P_2)\cdots\psi_4(P_8) \end{bmatrix}=\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \beta & \beta \\ \alpha & \beta & 0 & 1 & \alpha & \beta & \alpha & \beta \\ 0 & 0 & 1 & 1 & \beta & \beta & \alpha & \alpha \end{bmatrix}$$

进一步，如果把码 C 的全部码字找出来，我们便可发现 C 的最小距离为4，因此码 C 是一个 $(8,\ 4,\ 4)$ 线性码。

这一例子说明，我们确实能够利用代数曲线来构造线性码。这使我们为构造各种线性码找到了新的源泉，从而使编码理论的研究进入了一个全新的阶段。

今后，用 $\mathrm{Rat}(X)$ 代表（F_q 上的）不可约代数曲线 X 的有理函数全体所构成的有理函数域。$\mathrm{Rat}(X)$ 中的元素在射影曲线的情形下可表为两个同次多项式之比

$$f = A(x, y, z)/B(x, y, z)$$

并且如果另有 $f_1 = A_1(x, y, z)/B_1(x, y, z)$ 满足

$$f - f_1 \equiv 0 \pmod X$$

则 f 与 f_1 视为等同。注意此处 X 代表一个代数曲线。

例如，设 X 代表 F_2 上的不可约代数曲线

$$X = F(x, y, z) = y^2z + yz^2 + x^3 + x^2z$$

我们来计算 $f = (y^2 + yz)/xz$ 于点 $P = (0, 0, 1)$ 之值。注意到

$$\frac{y^2 + yz}{xz} - \frac{x^2 + xz}{z^2} \equiv 0 \pmod{F(x, y, z)}$$

故 $f = (y^2 + yz)/xz \equiv x(x + z)/z^2$ 于点 $P = (0, 0, 1)$ 之值 $f(P) = 0$。

对于 $\mathrm{Rat}(X)$ 中之元 f，若它的零点为 $\hat{P}_1, \cdots, \hat{P}_r$，相应的级数为 $n_1, \cdots, n_r$，而它的极点为 $q_1, \cdots, q_s$，相应的级数为 $m_1, \cdots, m_s$，则以 $\mathrm{div}(f)$ 代表形式和

$$(f) \triangleq \sum_{i=1}^{r} n_i \hat{P}_i - \sum_{j=1}^{s} m_j q_j \qquad (8\text{-}7)$$

称 (f) 为 f 的**除子**（divisor）。

例如，在例 8.2 中，对于 $\psi_2 = x/z$，我们有 $\mathrm{div}(\psi_2) = P_1 + P_2 - 2Q$。

§8.8 代数曲线中的一些重要概念

为了进一步介绍代数几何码，本节将引入代数曲线理论中的一些重要概念。需要说明的是，为了要严格地定义这些概念，必须深入介绍代数几何理论的进一步知识。限于篇幅及读者对象，我们在叙述这些概念时将不追求严格，并且尽量以实例说明。为

了易于理解，读者可将本节中讨论的有限域F_q的代数闭包$X=\overline{F}_q$想像成普通的复数域C。

一、局部环与局部参数

在本节中用K代表F_q的代数闭包$\overline{F}_q$。设X是一个仿射曲线或射影曲线，P是曲线X上的一点，$U(P)$是P点的一个邻域(为定义邻域概念，需在射影空间P^n或仿射空间A^n中引进所谓扎里斯基(Zariski)拓扑，此处从略)。在$U(P)$上定义的函数$\phi=f/g$称为于点P正则，如果$g(P)\neq 0$，其中f，g均为具有相同次数的齐次多项式。两个在点P正则的函数ϕ_1，ϕ_2称为是等价的，如果ϕ_1，ϕ_2在点P的某一邻域内相等。用$O(U)$代表在$U(P)$的每一点均为正则的函数全体，显然$O(U)$构成一个环。将$O(U)$中的函数按上述等价概念分类，又得到一个环，记为$O_p(X)$。

定义8.8.1 $O(U)$中正则函数等价类的集合所构成的环$O_P(X)$称为在X上点P的**局部环**(local ring)。

这里定义的局部环概念正是近世代数中的局部环概念。事实上，不难证明$O_P(X)$含有一个在点P等于0的函数类的集合，记为$m_P(X)$，它是$O_P(X)$中唯一的一个极大理想。建议读者作为练习证明这一结论。

在A^2中，若一曲线由$F(x, y)=0$定义，$P=(a, b)$是该曲线上一点。若偏导数$F_x(P)$与$F_y(P)$至少有一个不为0，则称点P为该曲线的非奇异点。这表明该曲线在点P有切线$F_x(P)(x-b)+F_y(P)(y-b)=0$。若曲线上每一点均为非奇异点，则称该曲线是**非奇异的**或**光滑的**。今后，我们总假定所讨论的曲线是光滑的。在一般情形下，如果m_P/m_P^2(作K—向量空间看待)具有维数1，则称相应的代数曲线在点P光滑。

因为m_P/m_P^2之维数为1，故该空间有一生成元t。我们同样也把t作为对应于m_P中之元。于是可以断定，$O_P(X)$中的每一元素z均可表为$z=ut^m$的形式，其中u是$O_P(X)$中的单位(即乘法可逆元)，m是某一整数。具备这一性质的元素t，作为

函数看待，称之为在点P的**局部参数**。如果$m>0$，则点P是z的m级零点；如果$m<0$，则点P是z的m级极点。我们引入记号

$$m=O_{rd^P}(z)=V_P(z)$$

对于一般在X上定义的有理函数$\phi=f/g$，我们可定义

$$V_P(f/g)=V_P(f)-V_P(g)$$

例8.3 假设曲线X是A^2中之圆$x^2+y^2-1=0$，且设$P=(1,\ 0)$。考虑$z=z(x,\ y)=1-x$，显然$z(P)=0$，因此$z\in m_P$。由于直线$y=0$与X的交点在点P的重数为1，故y即为局部参数。进一步，在X上我们有

$$z=1-x=\frac{y^2}{1+x}$$

而$(1+x)^{-1}$是$U_P(X)$的单位。因此$V_P(z)=2$。

如果在P^2中考虑上述例子，此时曲线X为$x^2+y^2-z^2=0$，$P=(1,\ 0,\ 1)$。我们考虑$U_P(X)$中的函数$(z-x)/z$，它也是m_P中之元素。于是在点P的局部参数为$t=y/z$。我们有

$$\frac{z-x}{z}=\frac{z^2-x^2}{z(z+x)}=\frac{y^2z}{z^2(z+x)}=t^2\frac{z}{z+x}$$

其中$z/(z+x)$是局部环$O_P(X)$中之单位。因此$V_P((z-x)/z)=2$

二、除子

除子的概念在代数几何中占有重要地位。

以下总假定X是K上的光滑射影曲线。

定义8.8.2 在曲线X上的有限个点所作的形式整系数线性组合

$$D=\sum_{P\in X}n_PP,\qquad n_P\text{是整数}\tag{8-8}$$

即除去X上的有限个点P外，$n_P=0$，称之为**除子**。如果式(8-8)中所有$n_P\geqslant 0$，则称除子D是有效的，记为$D\succ 0$。最

后，在式（8-8）中称$\sum n_P$为除子D的次数，记为

$$\deg(D)=\sum n_P$$

两个除子$D_1=\sum n_i P_i$及$D_2=\sum m_i P_i$可进行加减运算

$$D_1\pm D_2=\sum (n_i\pm m_i)P_i$$

例如，若$D_1=P_1+2P_2-P_3$，$D_2=P_1-3P_3+P_4$，则

$$D_1-D_2=2P_2+2P_3-P_4$$

因此，按上述的形式加法运算，X上定义的全部除子构成一个加法群（X上的自由阿贝尔群）。

定义8.8.3 X上全部除子所构成的加法群称为曲线X的除子群，记为$\mathrm{div}(X)$。

对于X上的有理函数f，在§8.7中已经定义过f的除子(f)。使用本节中的记号$V_P(\cdot)$，我们可以重新定义(f)如下：

定义8.8.4 对于X上的有理函数f，f不恒为0，定义f的除子为

$$(f)=\sum_{P\in X}V_P(f)P$$

对于$f=0$，我们规定

$$(f)=\sum_{P\in X}0P$$

在某种意义上说，函数f的除子可看作是一种登记表，它告诉我们这个函数在曲线X上有哪些零点与极点，以及它们相应的级数。因为f是分子与分母次数相同的有理函数，又因K是代数闭域，所以不难想象，f具有相同数目的零点与极点（连同其级数一起计算）。因此，直观上可看出下述定理成立。

定理8.8.1 （比索特（Bezout））对于X上的任一有理函数f，恒有$\deg(f)=0$。

现在，我们在除子群$\mathrm{div}(X)$上建立一种等价关系。设D，$D'\in\mathrm{div}(X)$，如果对于某一有理函数f，有$D-D'=(f)$，则

称除子D与D'线性等价，记为$D\cong D'$。不难证明，这确实是一个等价关系，即满足

（1） $D\cong D$

（2） $D\cong D'\Longrightarrow D'\cong D$

（3） $D\cong D'$，$D'\cong D''\Longrightarrow D\cong D''$

定义8.8.5 称商群$\mathrm{Div}(X)/\{(f)|f\in\mathrm{Rat}(X)\}$为曲线$X$的毕卡（Picard）群，记为

$$\mathrm{Pic}(X)=\mathrm{Div}(X)/\{(f)|f\in\mathrm{Rat}(X)\}$$

毕卡群也叫除子类群。

毕卡群在代数曲线理论中起着重要的作用。

类似于§8.6中用有理函数所构成的线性空间定义推广了的高帕码的情形一样，我们可在曲线X上做同样的事情。

设D为曲线X的一个除子。考察集合

$$\mathscr{L}(D)=\{f|f\in\mathrm{Rat}(X),\ f\neq 0,\ (f)+D\succ 0\}\cup\{0\}$$

如果设$D=\sum_{i=1}^{r}n_iP_i-\sum_{j=1}^{s}m_jQ_j$，所有$n_i$，$m_j$均$>0$。于是不难看出，$\mathscr{L}(D)$中的函数$f$，它或者为0，或者是以诸$Q_j$（$1\leqslant j\leqslant s$）至少为$m_j$级零点，并且除去可能以诸$P_i$（$1\leqslant i\leqslant r$）至多为$n_i$级极点外别无其它极点的有理函数。很明显，$\mathscr{L}(D)$构成一个域$K$上的线性空间。

定义8.8.6 设$D\in\mathrm{div}(X)$，称

$$\mathscr{L}(D)=\{f|f\in\mathrm{Rat}(X),\ f\neq 0,\ (f)+D\succ 0\}\cup\{0\}$$

为由曲线X的除子D所决定的线性空间。

可以证明，$\mathscr{L}(D)$必为有限维线性空间，以$\dim_k\mathscr{L}(D)$代表$\mathscr{L}(D)$的维数。我们有下面的定理。

定理8.8.2 对于线性空间$\mathscr{L}(D)$，下述性质成立：

（1） 若$\deg(D)<0$，则$\mathscr{L}(D)=\{0\}$

（2） $\dim_k\mathscr{L}(D)\leqslant 1+\deg(D)$

今后，用$l(D)$代表$\dim_k\mathscr{L}(D)$。$l(D)$与下一节要叙述的一个重要定理有直接的关系。

三、在曲线上的微分

讨论 A^2 上由方程 $F(x, y)=0$ 定义的曲线 X，且设 $P=(a, b)$ 为 X 上一点。曲线 X 在点 P 的切线 T_P 由 $d_PF=0$ 定义，其中 $d_P F$ 由下式定义：

$$d_PF=F_x(a, b)(x-a)+F_y(a, b)(y-b)$$

给定 $P\in X$，则映射 d_P 把每一个函数 F 变成一个线性函数 $d_P(F)$。同样，给定函数 F，则映射 d_PF 把每一点 $P\in X$ 皆变成一个线性函数 d_PF。

称线性算子 d_PF 为 F 在点 P 的微分。若考察每一点 $P\in X$ 的微分，则记为 dF。它具有下述性质：

（1） $d(F+G)=dF+dG$

（2） $da=0$， $a\in K$

（3） $d(FG)=FdG+GdF$

定义8.8.7 设 X 是闭域 K 上的仿射曲线。在 X 上定义 $\Omega(X)$ 为满足下述条件的集合：

$\Omega(X)$ 中的每一元素在每一点 $P\in X$ 的邻域 $U(P)$ 内均可表为 $\sum_{i=1}^{m} f_i dg_i$，其中 f_i，g_i 均在 $U(P)$ 正则，并且 dg_i 满足上述条件（1），（2），（3）。

称 $\Omega(X)$ 中的元素为**正则微分形式**。

利用正则微分形式容易建立有理微分形式概念。

定义8.8.8 考虑序偶 (U, ω) 与 (V, η)，ω，η 分别是邻域 U，V 上的正则微分形式。定义等价关系

$$(U, \omega)\sim(V, \eta)\Longleftrightarrow\omega=\eta \text{ 在 } U\cap V$$

按这一等价关系决定的等价类称为**有理微分形式**。

对于有理微分形式，我们有：$d(g/h)=(hdg-gdh)/h^2$，其中 g，$h\neq 0$。

从现在起，我们称 X 上的有理微分形式为微分。仍用 $\Omega(X)$ 代表这种微分的全体所成的空间。可以证明，$\Omega(X)$ 的维数为

1。因此，在具有局部参数 t 的点 P 的一个邻域内，微分 ω 可以表示成 $\omega = f\mathrm{d}t$ 的形式，其中 f 是有理函数。

定义8.8.9 微分 ω 的除子定义为

$$(\omega) = \sum_{P \in X} V_P(f_P)P$$

此处 $\omega = f_P\mathrm{d}t_P$ 是 ω 的局部表示。

可以证明除子（ω）的定义依赖于局部参数的选取，并且上面的和式仅有有限项系数不为 0 。

称 $W=(\omega)$ **为标准除子**。可以证明，这种标准除子构成毕卡群 Pic(X) 中的一个类。因此按定义 8.8.6，可以定义线性空间 $\mathscr{L}(W)$ 及其维数 $l\,(W)$。

定义8.8.10 设 X 为闭域 K 上的光滑射影曲线。称 $g = l\,(W)$ 为曲线 X 的**亏格**（genus）。

亏格是代数几何理论的重要概念。亏格是代数几何中内蕴的概念，而不是外在强加的。直观上说，这种流形在奇点附近形成若干个“洞”，这些“洞”的数目就是该流形的亏格。例如，拓扑学中已经指出，任何可定向的二维紧流形均同胚于一个具有若干环柄的球面（见图8-6）。这些环柄的个数 g，就是一个拓扑不变量，就是亏格。

下面的定理给出了计算曲线亏格的算法。

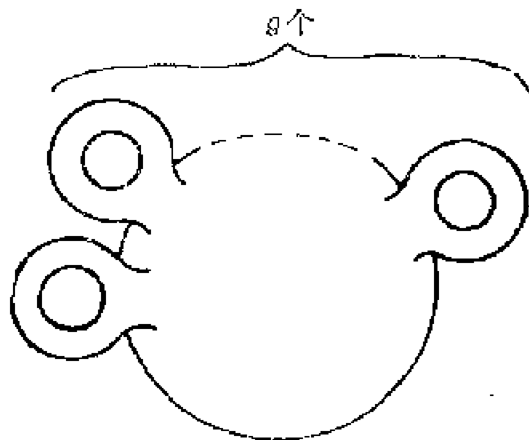

图 8-6

定理8.8.3 （普鲁克Plücker）公式）若X是P^2上一个光滑d次射影曲线，则

$$g=\frac{1}{2}(d-1)(d-2)$$

例如，若$X=P^1$，则$g=0$。由此可见，经典的高帕码就是利用亏格为0的射影直线构造的线性码。

为了在一般的代数曲线上构造高帕码，我们需要引进微分ω在点P的留数概念。

假设P是曲线X上一点，t是在点P邻域的局部参数，$\omega=f\mathrm{d}t$是ω的局部表示。于是函数f可展开成罗朗（Laurent）级数$\sum_{-\infty}^{\infty}a_it^i$。我们定义$\omega$在点$P$的留数为$a_{-1}$，记为

$$\mathrm{Res}_P(\omega)=a_{-1}$$

类似于复函数论中的留数定理，可以同样证明下述定理。

定理8.8.4 如果ω是光滑射影曲线X上的微分，则

$$\sum_{P\in X}\mathrm{Res}_P(\omega)=0$$

§8.9 黎曼-洛克(Riemann-Roch)定理

有了上一节的准备，我们便可介绍著名的黎曼-洛克定理了。

定理8.9.1 （黎曼-洛克）设D是亏格为g的光滑射影曲线上的一个除子。于是，对于任意标准除子W，有

$$l(D)-l(W-D)=\deg(D)-g+1$$

这一定理不但在代数几何及其相关的理论（诸如数论等）中占有中心地位，它同时也是在编码理论中获得具有重大意义的结果的关键所在。

利用这一定理，可以决定标准除子的次数。

推论8.9.1 对于标准除子W，有

$$\deg(W)=2g-2$$

证明 每一个在射影曲线上的正则函数均为常数，从而 $\mathscr{L}(0)=K$，$l(0)=1$。在定理8.9.1中置$D=W$，便可得到$\deg(W)=2g-2$。

〈证毕〉

推论8.9.2 设D是亏格为g的光滑射影曲线的除子，并且假设$\deg(D)>2g-2$。于是

$$l(D)=\deg(D)-g+1$$

证明 由推论8.9.1，$\deg(W-D)=\deg(W)-\deg(D)<(2g-2)-(2g-2)=0$。由定理8.8.2之（1），$\mathscr{L}(W-D)=\{0\}$，从而$l(W-D)=0$。再由定理8.9.1便得

$$l(D)=\deg(D)-g+1$$ 〈证毕〉

在定理8.9.1中之$l(W-D)$可用微分的概念加以解释。我们引进平行于定义8.8.6对于微分情形的相应概念。

定义8.9.1 设D为曲线X上的一个除子，我们定义

$$\Omega(D)=\{\omega\in\Omega(X);\ (\omega)-D\succ 0\}$$

并且用$\delta(D)$表示$\dim_k\Omega(D)$，称之为D的指标（index）。

可以证明

$$\delta(D)=l(W-D)$$

为了说明黎曼-洛克定理的应用，我们再回到§8.6中关于代数几何码的构造问题上来。

设X是F_q上的光滑射影曲线。设P_1，P_2，…，P_n为X上的有理点，并且D是除子$P_1+P_2+\cdots+P_n$。进一步，假设G是某一另外的除子，并且除子G由不同于诸P_i的有理点构成，并且满足条件

$$2g-2<\deg(G)<n \qquad (8\text{-}9)$$

定义8.9.2 在F_q上长为n的线性码$L(D,G)$是线性映射φ_L：$\mathscr{L}(G)\longrightarrow(F_q)^n$之下的像，$\varphi_L$由下式定义

$$\varphi_L(f)=(f(P_1),\ f(P_2),\ \cdots,\ f(P_n))$$

称这种码为广义的几何RS码。

定理8.9.2 $L(D, G)$码具有维数（信息位）$K=\deg(G)-g+1$及最小距离$d\geqslant n-\deg(G)$。

证明 （1）如果f属于映射φ_L之核$K_{er}\varphi_L=\{f\in\mathscr{L}(G)|\varphi_L(f)=0\}$，即$f(P_i)=0$，$(i=1, 2, \cdots, n)$。再注意到$f\in\mathscr{L}(G)$，则必有$f\in\mathscr{L}(G-D)$。由式（8-9），有$\deg(G-D)=\deg G-\deg D=\deg G-n<0$。因此，由定理8.8.2之（1），$\mathscr{L}(G-D)=\{0\}$，即$f=0$。这表明$\varphi_L$为$\mathscr{L}(G)$到$(F_q)^n$的单射。因此$l(G)=\dim_k\mathscr{L}(G)=L(D, G)$码的维数$K$。又由式（8-9）及推论8.9.2，得$l(G)=\deg G-g+1$。

（2）如果$\alpha(f)$具有重量d，则诸P_i中必有$n-d$个点P_{i_1}，P_{i_2}，$\cdots$，$P_{i_{n-d}}$，使$f(P_{i_k})=0$，$(k=1, 2, \cdots, n-d)$。因此，对于除子$E=P_{i_1}+\cdots+P_{i_{n-d}}$，必有$f\in\mathscr{L}(G-E)$（注意$f\in\mathscr{L}(G)$），从而$(f)+(G-E)\succ 0$，亦即

$$\deg(f)+\deg(G)-\deg(E)=\deg(G)-n+d\geqslant 0$$

此处由定理8.8.1，$\deg(f)=0$　　〈证毕〉

上述的广义的几何RS码，也称为第1类几何码，第2类几何码是所谓广义的几何高帕码，定义如下：

定义8.9.3 广义的几何高帕码是F_q上码长为n的线性码$L^*(D, G)$，它是线性映射

$$\varphi_L^*: \Omega(G-D)\longrightarrow(F_q)^n$$

之下的像，φ_L^*由下式定义：

$$\varphi_L^*(\eta)=(\mathrm{Res}_{P_1}(\eta), \mathrm{Res}_{P_2}(\eta), \cdots\mathrm{Res}_{P_n}(\eta))$$

线性码$L^*(D, G)$的相参数由下述定理给出。

定理8.9.3 线性码$L^*(D, G)$具有维数$K^*=n-\deg(G)+g-1$，最小距离$d^*\geqslant\deg(G)-2g+2$。

这一定理的证明与定理8.9.2类似，也是定理8.9.1的直接推论。请读者自己证明。

正如经典的高帕码与RS码的情形一样，我们有下述的定理。

定理8.9.4 $L(D, G)$ 与 $L^*(D, G)$ 互为对偶码。

证明 由定理8.9.2与定理8.9.3，$K+K^*=0$。因此只需证明 $L(D, G)$ 与 $L^*(D, G)$ 中的码字互为正交，即内积为0。设 $f\in\mathscr{L}(G)$，$\eta\in\Omega(G-D)$。由定义8.9.2与定义8.9.3可知，微分 $f\eta$ 除在点 P_1，P_2，…，P_n 可能有一级极点外，别无另外的极点，并且

$$\mathrm{Res}_{P_i}(f\eta)=f(P_i)\mathrm{Res}_{P_i}(\eta)$$

由定理8.8.4

$$\sum_{i=1}^{n} f(P_i)\mathrm{Res}_{P_i}(\eta)=0$$ 〈证毕〉

由前面的讨论可以看到，曲线 X 上有理点的个数与相应的线性码的码长有密切的关系。关于这一点我们介绍下述的著名结果。

定理8.9.5（威尔（Weil）界）设 X 是 F_q 上亏格为 g 的曲线，$N_q(X)$ 代表 X 上有理点的数目。于是有

$$|N_q(X)-(q+1)|\leqslant 2g\sqrt{q}$$

由上式可看出：

$$N_q(X)\leqslant q+1+[2g\sqrt{q}]$$

谢瑞（J.P.Serre）于1983年将此上界改进为

$$N_q(X)\leqslant q+1+g[2\sqrt{q}]$$

§8.10 椭圆曲线码

在本章之末，我们对椭圆曲线码做一大致的介绍。

亏格为1的平面代数曲线称为椭圆曲线。椭圆曲线 X 在 P^2 上的一般齐次表达式为

$$y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz^2+a_6z^3 \quad (8\text{-}10)$$

其中 a_1，a_2，a_3，a_4，$a_6\in F_q$。称

$$F(x, y, z)=y^2z+a_1xyz+a_3yz^2-x^3-a_2x^2z-a_4xz^2-a_6x^3$$

为威尔斯特拉斯（Weirstrass）多项式。

人们研究椭圆曲线的目的，在于它在有限域上能提供取之不尽的有限阿贝尔群。并且由于这种群的丰富结构，还是能够计算的。

有许多方式在椭圆曲线X上构造阿贝尔加法群。例如，取点$Q=(0,\ 1,\ 0)$（它在椭圆曲线上）作为加法单位元。如图8-7所示，对于曲线上任意两点P_1，P_2，设连结P_1，P_2两点的直线与该曲线相交于点R。若连结R，Q的直线与该曲线交于一点P_3，则定义$P_3=P_1\oplus P_2$。对于点P_1，P_2相重，或者有一个为Q，可类似地定义加法$\oplus$。对于曲线上的点P，我们还可以定义加法逆元P^*，满足$P\oplus P^*=Q$。因此曲线X上的点按上述加法运算$\oplus$构成加法群。不难看出，X上的有理点全体构成上述加法群的一个子群。例如，在§8.5中之例8.1中，$P_1=(0,\ \alpha,\ 1)$，从而$P_1^*=P_2=(0,\ \beta,\ 1)$。同理，$P_3^*=P_4$，$P_5^*=P_6$，$P_7^*=P_8$

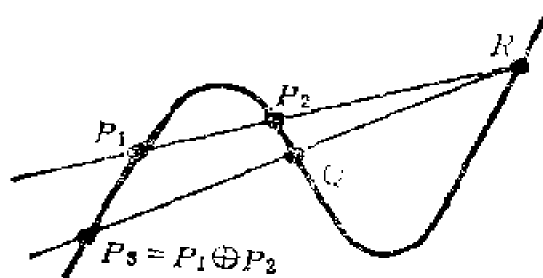

图 8-7

以椭圆曲线为底曲线构成的线性码，称为**椭圆曲线码**。

利用椭圆曲线上的有理点所构成的群，可以研究以椭圆曲线为底曲线所构成的线性码$L(D,\ G)$与$L^*(D,\ G)$的许多性质。

均可特（Y.Driencourt）等人于1987年曾证明，对于码长为n的椭圆曲线码$L(D,\ G)$，其最小距离d介于$n-\deg G$与$n-\deg G+1$之间（针对特征为2的域）

$$n-\deg G\leqslant d\leqslant n-\deg G+1$$

经验表明，当码长 n 不太大时，椭圆曲线码比 BCH 码的编码效率要高。表 8-2 针对 F_4 给出了这两种码的比较。表 8-2 中，n 为码长，d 为最小距离，r_0 代表 BCH 码的监督位数，r_1 代表椭圆曲线码的监督位数。

表 8-2

n	d	r_0	r_1
25	8	16	13
	10	19	17
81	12	33	23
	14	37	34
	16	45	37
289	18	61	49
	20	71	57
	26	91	61

关于椭圆曲线码的重量分布，覆盖半径，以及各种码界的研究，引起了不少学者的重视。

§8.11 结 束 语

代数几何码的研究是当代编码理论界关注的焦点之一。人们利用各种代数曲线试图构造性能及参数较好的线性码。从理论上探讨代数几何码的一般性质，讨论曲线上有理点的个数（与码长有关）及码界问题。对于代数几何码，编码问题比译码问题容易。为使代数几何码走向实用化，寻找高效率的译码算法，是这一领域中最为重要的课题。

编写本章的目的在于促进更多的读者了解代数几何码这一新兴的领域。当然，真正走向这一研究领域，需要一段艰苦的历程。代数几何码的出现，正如著名编码学家林特所指出的，它证明了一个重要的事实，任何数学，不管它多么高深，最终总是会在应用领域中放出异彩。

参 考 文 献

1 Berlekamp E R. Algebraic Coding Theory. McGraw-Hill Book Company, 1968.

2 Blahut R E. The Theory and Practice of Error-Control Codes. Addison-Wesley Publishing Company, 1983.

3 Goppa V D. Geometry and Codes. Kluwer Academic Publishers, 1988.

4 van Lint J H. Introduction to Coding Theory. Spinger-Verlag New York Inc., 1982.

5 MacWilliams F J and Sloane NJA. The Theory of Error-Correcting Codes. North-Holland Publishing Company, 1977.

6 Peterson W W and Weldon E J. Error-Correcting Codes. 2nd ed. M.I.T. Press, 1972.

7 Pless V. Introduction to the Theory of Error-Correcting Codes. John Wiley & Sons, Inc., 1982.

8 山西健司. 代数几何的符号理论. 数理科学, 1988, 9: 303.

9 万哲先. 代数和编码. 修订版. 北京: 科学出版社, 1980.

10 王新梅. 纠错码浅说. 北京: 人民邮电出版社, 1976.

11 王育民, 梁传甲. 信息与编码理论. 西安. 西北电讯工程学院出版社, 1986.

12 华罗庚. 数论导引. 北京: 科学出版社, 1975.

13 周炯槃. 信息理论基础. 北京: 人民邮电出版社, 1983.

14 〔美〕林舒. 纠错编码入门. 陈太一译. 北京: 人民邮电出版社, 1976.

15 〔荷〕范德瓦尔登. 代数学. 丁石孙等译. 北京: 科学出版社, 1978.

16 〔美〕贾柯勃逊. 抽象代数学. 黄缘芳译. 北京: 科学出版社, 1960.